ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Κβαντικοί υπολογιστικοί αλγόριθμοι για την παραγωγή ψευδοτυχαίων ακολουθιών

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Αικατερίνη Σ. Καλαϊτζάκη

Επιβλέπων : Γεώργιος Ματσόπουλος
Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούνιος 2024

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Κβαντικοί υπολογιστικοί αλγόριθμοι για την παραγωγή ψευδοτυχαίων ακολουθιών

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Αικατερίνη Σ. Καλαϊτζάκη

Επιβλέπων : Γεώργιος Ματσόπουλος
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 11/06/ 2024

.....	.....	.....
Γεώργιος Ματσόπουλος	Νικόλαος Ουζούνογλου	Ηρακλής Αβραμόπουλος
Καθηγητής Ε.Μ.Π.	Ομότιμος Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούνιος 2024

.....

Αικατερίνη Σ. Καλαϊτζάκη

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Περίληψη

Η παρούσα διπλωματική εργασία ασχολείται με την ανάπτυξη και εφαρμογή κβαντικών υπολογιστικών αλγορίθμων για την παραγωγή ψευδοτυχαίων ακολουθιών, εστιάζοντας ιδιαίτερα στην κβαντική εκδοχή των κλασικών Linear Feedback Shift Register (LFSR) γεννητριών. Οι κβαντικοί υπολογιστές, με τη δυνατότητά τους να επεξεργάζονται παράλληλα πολλαπλές καταστάσεις χάρη στην αρχή της υπέρθεσης, προσφέρουν νέα προοπτική στην παραγωγή ψευδοτυχαίων αριθμών που είναι κρίσιμη για εφαρμογές όπως η κρυπτογράφηση.

Αρχικά, η εργασία εισάγει τις βασικές αρχές των κβαντικών υπολογιστών και των χαρακτηριστικών τους, όπως η κβαντική υπέρθεση, η αβεβαιότητα και η κβαντική διεμπλοκή. Αυτές οι αρχές διαφοροποιούν ριζικά τους κβαντικούς υπολογιστές από τους κλασικούς, καθιστώντας τους ικανούς να επιλύουν προβλήματα με χρόνο και τρόπο που είναι πρακτικά αδύνατο να αντιμετωπιστούν με κλασικούς υπολογιστές. Στη συνέχεια, αναλύονται τα βασικά στοιχεία και οι λειτουργίες των κβαντικών υπολογιστών, συμπεριλαμβανομένων των qubits, των κβαντικών πυλών και των κβαντικών κυκλωμάτων.

Η κεντρική ιδέα της εργασίας επικεντρώνεται στην υλοποίηση της κβαντικής έκδοσης των LFSR γεννητριών. Οι LFSR γεννήτριες είναι συστήματα που χρησιμοποιούνται για την παραγωγή ψευδοτυχαίων ακολουθιών αριθμών και έχουν εφαρμογές στην κρυπτογράφηση και την επεξεργασία ψηφιακών σημάτων. Στην εργασία αυτή, αναπτύσσεται η θεωρητική βάση των κβαντικών LFSR, ενώ παράλληλα πραγματοποιείται προσομοίωση των κβαντικών αλγορίθμων σε πλατφόρμες όπως το Google Quantum AI.

Η μελέτη καταλήγει ότι η χρήση κβαντικών υπολογιστικών αλγορίθμων μπορεί να βελτιώσει σημαντικά την απόδοση και την ασφάλεια της παραγωγής ψευδοτυχαίων αριθμών, προσφέροντας μια αποδοτική και ασφαλή εναλλακτική στις κλασικές μεθόδους. Αυτή η εργασία αποτελεί ένα βήμα προς την κατεύθυνση της πρακτικής εφαρμογής των κβαντικών υπολογιστών σε πραγματικά προβλήματα και αναδεικνύει τις δυνατότητες των κβαντικών τεχνολογιών στην εξέλιξη της επιστήμης των υπολογιστών.

Λέξεις κλειδιά

Κβαντικοί υπολογιστές, Ψευδοτυχαίες ακολουθίες, Linear Feedback Shift Register (LFSR), Κβαντικοί αλγόριθμοι, Κβαντική υπέρθεση, Κβαντική διεμπλοκή, Qubits, Κβαντικές πύλες, Κβαντική προσομοίωση.

Abstract

This thesis focuses on the development and application of quantum computing algorithms for generating pseudorandom sequences, with a particular emphasis on the quantum version of classical Linear Feedback Shift Register (LFSR) generators. Quantum computers, with their ability to process multiple states in parallel thanks to the principle of superposition, offer new prospects for generating pseudorandom numbers, which is critical for applications such as cryptography.

Initially, the thesis introduces the fundamental principles of quantum computers and their characteristics, such as quantum superposition, uncertainty, and quantum entanglement. These principles fundamentally differentiate quantum computers from classical ones, enabling them to solve problems in ways and timescales that are practically impossible for classical computers. Subsequently, the basic elements and functions of quantum computers are analyzed, including qubits, quantum gates, and quantum circuits.

The central idea of the thesis focuses on implementing the quantum version of LFSR generators. LFSR generators are systems used for generating pseudorandom number sequences and have applications in cryptography and digital signal processing. This thesis develops the theoretical basis of quantum LFSR while simultaneously simulating quantum algorithms on platforms such as Google Quantum AI.

The study concludes that the use of quantum computing algorithms can significantly improve the performance and security of pseudorandom number generation, offering a efficient and secure alternative to classical methods. This work represents a step towards the practical application of quantum computers to real-world problems and highlights the potential of quantum technologies in advancing computer science.

Keywords

Quantum computers, Pseudorandom sequences, Linear Feedback Shift Register (LFSR), Quantum algorithms, Quantum superposition, Quantum entanglement, Qubits, Quantum gates, Quantum simulation.

Ευχαριστίες

Αρχικά θα ήθελα να ευχαριστήσω τον ομότιμο καθηγητή κ. Νικόλαο Ουζούνογλου και τον καθηγητή Γεώργιο Ματσόπουλο που μου έδωσαν την ευκαρία και να εκπονήσω την παρούσα διπλωματική εργασία και να εμβαθύνω τις γνώσεις μου στον τομέα της κβαντικής υπολογιστικής.

Μιας και η διπλωματική αυτή σηματοδοτεί το πέρας των φοιτητικών μου χρόνων θα ήθελα να ευχαριστήσω την οικογένεια μου, τους γονείς μου Άρτεμις και Στέλιο και την αδερφή μου Μυρτώ για την στήριξη, την κατανόηση και την αμέριστη αγάπη που μου έδειξαν όλα αυτά τα χρόνια, που στάθηκαν δίπλα στις εύκολες αλλά πόσο μάλλον στις δύσκολες στιγμές και με βοήθησαν να φτάσω εδώ.

Θα ήθελα επίσης να ευχαριστήσω τους φίλους και συμφοιτητές μου, την Έλενα και τη Νατάσα που έκαναν αυτά τα χρόνια ακόμα όμορφα και ξέγνοιαστα.

Δε θα μπορούσα να μην ευχαριστήσω τους ΑΝεξάρτητους Αριστερούς Φοιτητές Ηλεκτρολόγους, εκείνα τα παιδιά στα τραπεζάκια, που πάντα παλεύουν για το δίκιο των πολλών. Ευχαριστώ, λοιπόν, τους ΑΝ.Α.Φ.Η. αλλά και όλους εκείνους τους συντρόφους που χάρη σε αυτούς βλέπω τον κόσμο με αλλά μάτια. Τους ευχαριστώ μέσα από την καρδιά μου γιατί μαζί τους γνώρισα την συντροφικότητα, και με έμαθαν να μην σκύβω το κεφάλι και ακόμα και στους πιο δύσκολους καιρούς να μάχομαι και να μην τα παρατάω. Που σε πείσμα των καιρών, με το βλέμμα και τη γροθιά υψωμένη γράφουν ιστορία στους δρόμους.

≪Κι όχι να πείτε που `κανα και τίποτα σπουδαίο, μόνο που πόνεσα μαζί σας κι ονειρεύτηκα μαζί σας. Μόνο που σε βρήκα και με βρήκες σύντροφε.≫ Γ.Ρίτσος

Κατερίνα Καλαϊτζάκη

Αθήνα, Ιούνιος 2024

Περιεχόμενα

1. Εισαγωγή

1. 1. Εισαγωγή στους Κβαντικούς Υπολογιστές

Στην εποχή της συνεχούς τεχνολογικής προόδου, η κβαντική υπολογιστική αναδεικνύεται ως ένας από τους πλέον ελπιδοφόρους και πρωτοποριακούς τομείς. Η κβαντική υπολογιστική, αντλώντας αρχές από την κβαντική φυσική, εισάγει μια νέα παράδοση στον τρόπο που επεξεργαζόμαστε πληροφορίες. Το θεμέλιο της λειτουργίας ενός κβαντικού υπολογιστή εδράζεται στις αρχές της κβαντομηχανικής, κάτι που του επιτρέπει να εκτελεί υπολογισμούς με έναν τρόπο που διαφέρει ριζικά από αυτόν ενός παραδοσιακού υπολογιστή που λειτουργεί βάσει των αρχών της κλασικής φυσικής. Ένα εκ των κυριότερων πλεονεκτημάτων του κβαντικού υπολογιστή είναι η ικανότητά του να εκτελεί πολλαπλούς υπολογισμούς παράλληλα χάρη στην κατάσταση της κβαντικής υπέρθεσης, δηλαδή την ικανότητά του να βρίσκεται σε πολλαπλές καταστάσεις ταυτοχρόνως. Σε σύγκριση με τα παραδοσιακά ψηφιακά υπολογιστικά συστήματα, τα κβαντικά υπολογιστικά συστήματα προσφέρουν τη δυνατότητα να μειώσουν δραματικά τόσο τον χρόνο εκτέλεσης όσο και την κατανάλωση ενέργειας.

Η κβαντική υπολογιστική στηρίζεται στις δομικές αρχές της κβαντομηχανικής, η οποία ασχολείται με τον μικρόκοσμο των βασικών σωματιδίων όπως τα ηλεκτρόνια και τα φωτόνια. Ωστόσο, η συμπεριφορά στον υποατομικό κόσμο είναι ουσιαστικά ασυνήθιστη και διαφορετική από την καθημερινή μας εμπειρία του φυσικού κόσμου. Γι αυτό τις περισσότερες φορές οι κβαντικοί υπολογισμοί υπερβαίνουν τα κοινά δεδομένα της λογικής και της συνηθισμένης σκέψης.

1.2. Αρχή της αβεβαιότητας

Η αρχή της αβεβαιότητας, που διατυπώθηκε από τον Werner Heisenberg, αποτελεί έναν πυλώνα της κβαντικής μηχανικής και εκφράζει μια θεμελιώδη χαρακτηριστική του κβαντικού κόσμου. Το κύριο διακριτό στοιχείο που ξεχωρίζει την κβαντική από την κλασική φυσική είναι η Αρχή της Αβεβαιότητας ή Απροσδιοριστίας. Αντίθετα με την κλασική φυσική, όπου οι αβεβαιότητες στις μετρήσεις προκύπτουν από τυχόν σφάλματα των μετρητικών οργάνων, στην κβαντομηχανική η αβεβαιότητα είναι ένα φυσικό και αναπόφευκτο φαινόμενο. Αυτή η αρχή υποδηλώνει ότι δεν είναι δυνατή η ταυτόχρονη μέτρηση ορισμένων ζευγών φυσικών μεγεθών, όπως η θέση και η ορμή ενός σωματιδίου, με απόλυτη ακρίβεια. Η μαθηματική εκφρασή της αρχής:

$$\Delta x * \Delta p \geq \hbar/2,$$

όπου Δx και Δp συμβολίζουν τις αβεβαιότητες στην θέση και την ορμή αντίστοιχα, και ħ είναι η σταθερά του Planck διαιρεμένη με 2π, δηλώνει ότι η αύξηση της ακρίβειας στη μέτρηση του ενός μεγέθους συνεπάγεται μείωση της ακρίβειας στη μέτρηση του άλλου. Η αρχή της αβεβαιότητας έχει βαθιές συνέπειες για την κατανόηση της φύσης του κβαντικού κόσμου, αποκαλύπτοντας ότι

η πραγματικότητα στο μικροσκοπικό επίπεδο δεν είναι τόσο καθορισμένη όσο στον μακροσκοπικό κόσμο της κλασικής φυσικής.

1.3. Αρχή της Υπέρθεσης

Στον κόσμο της κβαντικής μηχανικής, η αρχή της υπέρθεσης αποτελεί μία εκ των πλέον θεμελιωδών ιδιοτήτων, η οποία ριζικά διαφοροποιεί την κβαντική από την κλασική φυσική. Η υπέρθεση επιτρέπει σε ένα κβαντικό σώμα, όπως το qubit, να βρίσκεται ταυτόχρονα σε πολλαπλές καταστάσεις. Αυτό σημαίνει ότι αντί να είναι περιορισμένο σε μία μόνο δυαδική κατάσταση (0 ή 1), όπως συμβαίνει με τα κλασικά bits, ένα qubit μπορεί να βρίσκεται σε ένα συνδυασμό των δύο, παρέχοντας μια κυματική αναπαράσταση που ενσωματώνει πληθώρα πιθανών καταστάσεων. Αυτή η ιδιότητα είναι όχι μόνο θεμελιώδης για την κατανόηση της κβαντικής συμπεριφοράς, αλλά αποτελεί και τον κρίσιμο παράγοντα που ενισχύει την υπολογιστική ισχύ των κβαντικών υπολογιστών. Η δυνατότητα ενός κβαντικού συστήματος να επεξεργάζεται πολλαπλές καταστάσεις παράλληλα δημιουργεί την προοπτική για την ταχύτερη και πιο αποτελεσματική επίλυση σύνθετων υπολογιστικών προβλημάτων, ανοίγοντας νέους δρόμους στην τεχνολογική πρόοδο.

Η κβαντική αρχή της υπέρθεσης υποστηρίζει ότι ένα κβαντικό σύστημα μπορεί να βρίσκεται ταυτόχρονα σε μια συνδυασμένη κατάσταση όλων των πιθανών κλασικών καταστάσεων, με κάθε κατάσταση να έχει έναν μιγαδικό συντελεστή. Ας θεωρήσουμε ένα σύστημα με k διακριτές καταστάσεις. Η βασική κατάσταση ενός συστήματος συμβολίζεται ως |0⟩, και οι επόμενες καταστάσεις ως |1⟩ μέχρι |k − 1⟩, ο συμβολισμός αυτός ονομάζεται ket. Μια τυπική κβαντική κατάσταση θα εκφράζεται ως $a_0|0\rangle+a_1|1\rangle+...+ a_{k-1} |k - 1\rangle$, όπου οι συντελεστές a_0, a1, ..., ak−1 είναι μιγαδικοί αριθμοί που ικανοποιούν τη συνθήκη$\sum_{i=0}^{k-1} |a_i|^2 = 1$. Κάθε συντελεστής ai αποτελεί το πλάτος της αντίστοιχης κατάστασης |i⟩.

1.4. Αρχή της μέτρησης

Η αρχή της μέτρησης στην κβαντομηχανική είναι ένας θεμελιώδης κανόνας που καθορίζει πώς η παρατήρηση επηρεάζει και καθορίζει την κατάσταση ενός κβαντικού συστήματος. Αυτή η αρχή υποστηρίζει ότι ένα κβαντικό σωματίδιο, όπως το ηλεκτρόνιο ή το φωτόνιο, δεν έχει μια συγκεκριμένη ιδιότητα ή κατάσταση μέχρι να γίνει η μέτρηση. Μέχρι εκείνη τη στιγμή, το σωματίδιο βρίσκεται σε μια κατάσταση υπέρθεσης, όπου διάφορες πιθανές καταστάσεις συνυπάρχουν παράλληλα. Κατά την μέτρηση, η κυματοσυνάρτηση του σωματιδίου 'καταρρέει', και το σωματίδιο αποκτά μια συγκεκριμένη κατάσταση από το φάσμα των πιθανών καταστάσεων. Αυτό το φαινόμενο έχει σημαντικές συνέπειες στην κατανόηση της κβαντικής συμπεριφοράς, αφού υποδηλώνει ότι η πραγματικότητα σε κβαντικό επίπεδο δεν είναι απολύτως καθορισμένη

μέχρι να πραγματοποιηθεί μια παρατήρηση. Αυτή η κατάρρευση της κυματοσυνάρτησης αναδεικνύει την περίπλοκη αλληλεπίδραση μεταξύ παρατηρητή και συστήματος στον κβαντικό κόσμο.

Η κβαντική κατάσταση $|\phi\rangle = \sum_{i=0}^{k-1} a_i|i\rangle$ βρίσκεται στην ιδιωτική σφαίρα του ηλεκτρονίου, με περιορισμένη δυνατότητα πρόσβασης στις πληροφορίες της. Μια μέτρηση σε ένα σύστημα με k καταστάσεις παρέχει τον αριθμό i ως αποτέλεσμα με πιθανότητα $|a_i|^2$

Τα αποτελέσματα μιας μέτρησης, λοιπόν, είναί πιθανοκρατικά. Με λίγα λόγια στην κβαντική μηχανική, ακόμα και αν γνωρίζουμε πλήρως την κβαντική κατάσταση ενός συστήματος (περιγραφόμενη από ένα κυματοσυναρτησιακό ή διάνυσμα στον χώρο Hilbert), δεν μπορούμε να προβλέψουμε με απόλυτη ακρίβεια το αποτέλεσμα μιας μέτρησης. Αντ' αυτού, μπορούμε να προσδιορίσουμε μόνο τις πιθανότητες για τα διάφορα δυνατά αποτελέσματα. Ένας σημαντικός παράγοντας της μέτρησης είναι η επίδρασή της στην κατάσταση του συστήματος. Έτσι, αμέσως μετά από μια μέτρηση, το σύστημα βρίσκεται στην κατάσταση που εντοπίστηκε. Αυτό σημαίνει ότι δεν μπορούμε να λάβουμε περαιτέρω πληροφορίες για τα πλάτη a_i επαναλαμβάνοντας τη μέτρηση αμέσως μετά.

1.5. Χώρος Hilbert

Η γεωμετρία του χώρου Hilbert αποτελεί έναν κρίσιμο θεμελιώδη πυλώνα στην κβαντική μηχανική και, κατ' επέκταση, στους κβαντικούς υπολογιστές. Για να κατανοήσουμε τον ρόλο της, ας εξετάσουμε πρώτα τι είναι ο χώρος Hilbert και πως συνδέεται με την κβαντική φυσική.

Ο χώρος Hilbert είναι ένας αφηρημένος, μαθηματικά ορισμένος χώρος που χρησιμοποιείται στην κβαντική φυσική. Είναι ένας απειροδιάστατος διανυσματικός χώρος. Σε αυτόν τον χώρο, οι καταστάσεις ενός κβαντικού συστήματος αναπαρίστανται ως διανύσματα. Ο χώρος του Hilbert είναι πλήρης χώρος, που σημαίνει ότι κάθε ακολουθία των στοιχείων του χώρου που συγκλίνει, συγκλίνει σε ένα στοιχείο εντός του ίδιου χώρου.

Η κατάσταση ενός κβαντικού συστήματος (π.χ. ενός ηλεκτρονίου) περιγράφεται από ένα διάνυσμα σε έναν χώρο Hilbert. Αυτό το διάνυσμα αντιπροσωπεύει τη γραμμική υπέρθεση των διαφορετικών κβαντικών καταστάσεων που μπορεί να βρίσκεται το σύστημα. Μπορούμε λοιπόν να αναπαραστήσουμε την κατάσταση ενός συστήματος με k καταστάσεις ως ένα διάνυσμα k διαστάσεων. $|\psi\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{k-1} \end{pmatrix}$

Θέτουμε τις κβαντικές καταστάσεις ως τα παρακάτω διανύσματα:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \ldots, |k-1\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

Οι k διαφορετικές κλασικές καταστάσεις που συμβολίζονται ως $|0\rangle$, $|1\rangle$, ..., $|k-1\rangle$, απεικονίζονται μέσω k διανυσμάτων που είναι μοναδιαία και ορθογώνια ανα δύο μεταξύ τους. Αυτό σημαίνει ότι αυτά τα διανύσματα σχηματίζουν μια βάση σε έναν k-διάστατο μιγαδικό διανυσματικό χώρο.

Το εσωτερικό γινόμενο στο χώρό Hilbert για $|\phi\rangle = \sum_{i=0}^{k-1} a_i|i\rangle$ και $|\psi\rangle = \sum_{i=0}^{k-1} b_i|i\rangle$ ορίζεται ως

$$\langle \phi, \psi \rangle = \sum_{i=0}^{k-1} a_i^* \, b_i$$

Όπου a_i^*, ο συζηγής μιγαδικός του a_i

1.6. Κβαντική Διεμπλοκή

Η κβαντική διεμπλοκή (entanglement) είναι ένα από τα πιο παράδοξα και εντυπωσιακά φαινόμενα στην κβαντική μηχανική. Δύο ή περισσότερα σωματίδια θεωρούνται "κβαντικά διεμπλεκόμενα" όταν η κβαντική κατάσταση του ενός δεν μπορεί να περιγραφεί ανεξάρτητα από την κατάσταση του άλλου, ακόμη και όταν τα σωματίδια βρίσκονται σε μακρινή απόσταση. Σε ένα διεμπλεκόμενο σύστημα, οι ιδιότητες (το σπιν, η θέση, η κινητική ενέργεια) των σωματιδίων είναι συσχετισμένες. Αυτό σημαίνει ότι η μέτρηση μιας ιδιότητας στο ένα σωματίδιο καθορίζει αυτομάτως την αντίστοιχη ιδιότητα του άλλου, ανεξάρτητα από την απόσταση που τα χωρίζει. Συνεπώς γνωρίζοντας την τιμή του ενός, θα γνωρίζουμε αυτόματα και την τιμή του άλλου. Η διεμπλοκή έχει προταθεί ως μέθοδος για κβαντική επικοινωνία και κβαντική κρυπτογράφηση. Στην κβαντική επικοινωνία, η πληροφορία μεταδίδεται μέσω της κατάστασης των διεμπλεκόμενων σωματιδίων, ενώ στην κβαντική κρυπτογράφηση, η διεμπλοκή χρησιμοποιείται για να εξασφαλίσει την ασφάλεια της μεταφοράς της πληροφορίας. Μέσω της κβαντικής διεμπλοκής σε ένα κβαντικό υπολογιστή μπορούμε να έχουμε δύο qubit στα οποία η πληροφορία του ενός θα μεταφέρεται και θα επηρεάζει αμέσως το άλλο.

2. Κβαντικός Υπολογιστής-Βασικά Στοιχεία και Λειτουργίες

2.1. Κβαντικός Υπολογιστής

Ο κβαντικός υπολογιστής είναι μια υπολογιστή μηχανή που χρησιμοποιεί τις αρχές της κβαντικής μηχανικής για την επεξεργασία πληροφοριών. Σε αντίθεση με τους κλασικούς υπολογιστές, οι οποίοι χρησιμοποιούν bits για την αναπαράσταση της πληροφορίας ως 0 ή 1, οι κβαντικοί υπολογιστές χρησιμοποιούν κβαντικά bits ή qubits. Η ιστορία των κβαντικών υπολογιστών είναι σχετικά πρόσφατη και συνδέεται άμεσα με την εξέλιξη της κβαντικής φυσικής και της υπολογιστικής τεχνολογίας. Η ιδέα της κβαντικής υπολογιστικής άρχισε να διαμορφώνεται από τις δεκαετίες του '60 και '70, με τον Richard Feynman και τον Yuri Manin να είναι από τους πρώτους που πρότειναν την χρήση κβαντικών φαινομένων στους υπολογισμούς. Στις αρχές της δεκαετίας του 1990, οι ερευνητές άρχισαν να αναπτύσσουν τους πρώτους κβαντικούς αλγορίθμους. Ο πιο γνωστός είναι ο αλγόριθμος του Peter Shor (1994), ο οποίος μπορεί να διασπάσει πολύ μεγάλους αριθμούς σε πρώτους παράγοντες πολύ πιο γρήγορα από οποιονδήποτε κλασικό αλγόριθμο. Στις αρχές των 2000, άρχισε η ανάπτυξη πειραματικών κβαντικών υπολογιστών. Στη δεκαετία του 2010, η τεχνολογία κβαντικών υπολογιστών άρχισε να εξελίσσεται με γρήγορους ρυθμούς. Εταιρείες όπως η Google, η IBM και άλλες άρχισαν να αναπτύσσουν πιο προηγμένους κβαντικούς υπολογιστές. Το 2019, η Google ανακοίνωσε ότι είχε επιτύχει την "κβαντική υπεροχή", ισχυριζόμενη ότι ένας από τους κβαντικούς υπολογιστές της είχε λύσει ένα πρόβλημα που θα ήταν αδύνατο για έναν κλασικό υπολογιστή. Αν και αυτό το επίτευγμα δεν έχει άμεση πρακτική εφαρμογή, θεωρείται κρίσιμο για την εξέλιξη των κβαντικών υπολογιστών προς την επίλυση πραγματικών προβλημάτων.

Σε σύγκριση με τα κλασικά ψηφιακά υπολογιστικά συστήματα, τα κβαντικά συστήματα υπολογισμού παρέχουν την ευκαιρία να μειώσουν σημαντικά τόσο τον απαιτούμενο χρόνο επεξεργασίας όσο και την ενεργειακή κατανάλωση. Το γεγονός αυτό καθιστά τους κβαντικούς υπολογιστές ένα σημαντικό τομέα έρευνας και ανάπτυξης. Οι προκλήσεις που πρέπει να αντιμετωπιστούν περιλαμβάνουν την βελτίωση της σταθερότητας των qubits, την μείωση των σφαλμάτων και την αύξηση της κλίμακας των κβαντικών κυκλωμάτων. Η επιτυχία σε αυτούς τους τομείς θα μπορούσε να οδηγήσει σε πιο ισχυρούς κβαντικούς υπολογιστές με ευρύ φάσμα εφαρμογών. Η εξέλιξη των κβαντικών υπολογιστών αντιπροσωπεύει ένος σημαντικό βήμα προς τα εμπρός στην υπολογιστική τεχνολογία και έχει το δυναμικό να επιφέρει σημαντικές αλλαγές σε πολλούς τομείς, από την κρυπτογραφία και την ασφάλεια δεδομένων μέχρι την ανάπτυξη νέων φαρμάκων και υλικών.

2.2. Qubit

Τα qubits, ή κβαντικά bits, αποτελούν τη θεμελειώδη μονάδα πληροφορίας στην κβαντική υπολογιστική και λειτουργούν βασιζόμενα στις αρχές της κβαντικής μηχανικής. Ενώ ένα κλασικό bit στους συμβατικούς υπολογιστές μπορεί να βρίσκεται σε μία από δύο καταστάσεις, 0 ή 1, ένα qubit μπορεί να υπάρχει σε μια υπέρθεση καταστάσεων, συνδυάζοντας τόσο το 0 όσο και το 1 ταυτόχρονα. Αυτό επιτρέπει στα qubits να αποθηκεύσουν και να επεξεργαστούν πολύ μεγαλύτερες ποσότητες πληροφορίας σε σύγκριση με τα κλασικά bits.

Ένα qubit είναι ένα δυσδιάστατο κβαντικό σύστημα και η κατάσταση του μπορεί να εκφραστεί ως:

$$|\psi\rangle = a|0\rangle + \beta|1\rangle$$

όπου α, β μιγαδικοί αριθμοί με $|\alpha|^2 + |\beta|^2 = 1$ και $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$ $και$ $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$

Σε αντιδιαστολή με ένα bit, η μέτρηση της κατάστασης ενός qubit οδηγεί στην αλλαγή της, σύμφωνα με την αρχή της μέτρησης. Όταν μετράμε ένα qubit, που η κατάστασή του περιγράφεται από την παραπάνω εξίσωση, το αποτέλεσμα θα είναι είτε η τιμή 0 με πιθανότητα $|\alpha|^2$ είτε η τιμή 1 με πιθανότητα $|\beta|^2$.

2.3. Σφαίρα του Bloch

Η Σφαίρα του Bloch είναι ένας γεωμετρικός τρόπος αναπαράστασης της κατάστασης ενός qubit στην κβαντική υπολογιστική. Αντιπροσωπεύει την κβαντική κατάσταση του qubit ως ένα σημείο στην επιφάνεια μιας σφαίρας. Η κατάσταση του qubit αναπαρίσταται από το διάνυσμα από το κέντρο της σφαίρας προς αυτό το σημείο. Ο «βόρειος» και ο «νότιος» πόλος της σφαίρας αντιστοιχούν στις κλασικές καταστάσεις 0 και 1 αντίστοιχα. Τα σημεία που βρίσκονται μεταξύ των πόλων αναπαριστούν καταστάσεις υπέρθεσης, όπου το qubit είναι ένας συνδυασμός των 0 και 1. Η ακριβής θέση στη σφαίρα δείχνει τη σχετική πιθανότητα του qubit να βρεθεί στην κατάσταση 0 ή 1 όταν μετρηθεί. Οποιαδήποτε κίνηση του σημείου αυτού στην επιφάνεια της σφαίρας αντιστοιχεί σε μια αλλαγή στην κβαντική κατάσταση του qubit. Η Σφαίρα του Bloch, παρέχει έναν ισχυρό και οπτικό τρόπο για να κατανοήσουμε τις κβαντικές λειτουργίες, της λειτουργίες των κβαντικών πυλών και τις αλλαγές στην κατάσταση ενός qubit.

2.4 Κβαντικά συστήματα μεγαλύτερη διάστασης

Παραπάνω αναλύσαμε τον χώρο καταστάσεων ενός qubit. Τι συμβαίνει όμως όταν έχουμε παραπάνω qubits. Ας πάρουμε για παράδειγμα τι συμβαίνει όταν έχουμε δύο qubits. Αρχικά, χρειάζεται να διευρύνουμε τον χώρο καταστάσεων για να μπορέσουμε να αναλύσουμε μεγαλύτερο πλήθος Qubits. Για παράδειγμα, αν έχουμε δύο Qubits σε αυτές τις καταστάσεις:

$$|\psi 1\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

$$|\psi 2\rangle = \gamma\,|0\rangle + \delta\,|1\rangle$$

Ο χώρος που απαιτείται για να περιγράψουμε αυτό το σύστημα θα είναι τετραδιάστατος (4 = 2×2). Η συνολική κατάσταση του συστήματος ορίζεται από το τανυστικό γινόμενο των δύο διανυσμάτων.

$$|\psi\rangle = |\psi 1\rangle \otimes |\psi 2\rangle$$

Όπου το τανυστικό γινόμενο ορίζεται ως $\begin{pmatrix}\alpha\\ \beta\end{pmatrix} \otimes \begin{pmatrix}\gamma\\ \delta\end{pmatrix} = \begin{pmatrix}\alpha\gamma\\ \alpha\delta\\ \beta\gamma\\ \beta\delta\end{pmatrix}$

Τα διανύσματα βάσης του χώρου καταστάσεων δύο qubits είναι τα εξής

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}$$

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}$$

$$|11\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

Ας δούμε τώρα τι συμβαίνει όταν έχουμε n qubits. Το τανυστικό γινόμενο n δισδιάστατων διανυσμάτων ορίζεται ως εξής:

$$\binom{\alpha_1}{\beta_1} \otimes \binom{\alpha_2}{\beta_2} \otimes \cdots \otimes \binom{\alpha_n}{\beta_n} = \begin{pmatrix} a_1 a_2 \dots a_{n-1} a_n \\ a_1 a_2 \dots a_{n-1} \beta_n \\ \vdots \\ \beta_1 \beta_2 \dots \beta_{n-1} a_n \\ \beta_1 \beta_2 \dots \beta_{n-1} \beta_n \end{pmatrix}$$

Ανάλογα ορίζουμε και την βάση του χώρου:

$$|0 \cdots 0\rangle = |0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$|0 \cdots 1\rangle = |0\rangle \otimes |0\rangle \otimes \cdots \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}$$

$$\vdots$$

$$|1 \cdots 0\rangle = |1\rangle \otimes |1\rangle \otimes \cdots \otimes |0\rangle = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ 0 \end{pmatrix}$$

$$|1 \cdots 1\rangle = |1\rangle \otimes |1\rangle \otimes \cdots \otimes |1\rangle = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

Σύμφωνα με τα διανύσματα βάσης που ορίσαμε παραπάνω, η κάθε κατάσταση του κβαντικού συστήματος γράφεται ως γραμμικός συνδυασμός των διανυσμάτων βάσης.

$|\psi\rangle = \sum_{i=0}^{2^n-1} c_i |b_i\rangle$ με $\sum_{i=0}^{2^n-1} |c_i|^2 = 1$

2.5 Κβαντικοί καταχωρητές

Οι κβαντικοί καταχωρητές (quantum registers) αποτελούν έναν βασικό συστατικό στην κβαντική υπολογιστική και αντιπροσωπεύουν τον τρόπο με τον οποίο αποθηκεύονται και χειρίζονται οι πληροφορίες σε ένα κβαντικό υπολογιστή. Ενας κβαντικός καταχωρητής αποτελείται από μια σειρά από qubits. Κάθε qubit σε έναν κβαντικό καταχωρητή μπορεί να βρίσκεται σε κατάσταση υπέρθεσης. Μέσω της εμπλοκής, οι καταστάσεις των qubits μπορούν να συνδεθούν με τρόπους που δεν είναι δυνατοί στα κλασικά συστήματα υπολογιστών. Η δυνατότητα των κβαντικών καταχωρητών να υπάρχουν σε πολλαπλές καταστάσεις ταυτόχρονα οδηγεί σε τεράστια αύξηση της υπολογιστικής ισχύος. Για παράδειγμα, ενώ ένας κλασικός καταχωρητής με n bits μπορεί να

αντιπροσωπεύει μια κατάσταση σε κάθε χρονική στιγμή, ένας κβαντικός καταχωρητής με n qubits μπορεί να αντιπροσωπεύει 2^n καταστάσεις ταυτόχρονα. Ένας καταχωρητής n qubits, λοιπόν, βρίσκεται σε μία κατάσταση η οποία είναι ένα διάνυσμα του χώρου $\mathbb{C}^{2^n}$και είναι υπέρθεση των 2^n καταστάσεων$|00 \ldots 0\rangle$, $|00 \ldots 1\rangle$, … , $|11 \ldots 1\rangle$.

2.6 Κβαντικές πύλες

2.6.1. Κβαντικές πύλες μιας εισόδου

Στα κβαντικά συστήματα, η εξέλιξη μέσα στο χρόνο συμβαίνει μέσω μιας διαδικασίας που διατηρεί τη μοναδικότητα και την ορθογωνιότητα του συστήματος, δηλαδή ενός ορθομοναδιαίου μετασχηματισμού. Αν το εξετάσουμε γεωμετρικά, αυτός ο μετασχηματισμός αντιστοιχεί σε μια περιστροφή στον χώρο Hilbert. Αυτό σημαίνει ότι το μέγεθος του διανύσματος κατάστασης παραμένει σταθερό. Ένας μοναδιαίος μετασχηματισμός περιγράφεται από έναν πίνακα U με μιγαδικές τιμές. Ο πίνακας U ονομάζεται μοναδιαίος εάν

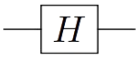
$$\mathrm{U}U^{\dagger} = U^{\dagger}\mathrm{U} = \mathrm{I}.$$

Όπου $U^{\dagger}$: ο ανάστροφος συζηγείς του U

Κάθε κβαντική πύλη μπορεί να αναπαρασταθεί ως ένας ορθομοναδιαίος μετασχηματισμός. Αυτό σημαίνει πως ο αριθμός των qubits εισόδου ισούται με τον αριθμό των qubits εξόδου. Επίσης κάθε πύλη είναι αναστρέψιμη, πράγμα που σημαίνει ότι η αρχική κατάσταση των qubits μπορεί να ανακτηθεί μέσω της αντίστροφης λειτουργίας. Ας δούμε τις βάσικες κβαντικές πύλες και πως αυτές επιδρούν σε ένα qubit.

- Πύλη Hadamard:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$



Η πύλη Hadamard είναι ένα εξαιρετικά σημαντικό εργαλείο στην κβαντική υπολογιστική. Χρησιμοποιείται ευρέως λόγω της ικανότητάς της να δημιουργεί υπέρθεση, Όταν ένα qubit είναι σε μια κατάσταση υπέρθεσης δημιουργημένη από την πύλη Hadamard, και το μετρήσουμε, υπάρχει ίση πιθανότητα (50% για κάθε περίπτωση) το αποτέλεσμα να είναι είτε 0 είτε 1.

- Πύλη περιστροφής:

$$R_{\theta} = \begin{pmatrix} cos\theta & -sin\theta \\ sin\theta & cos\theta \end{pmatrix}$$

Η λειτουργία της πύλης R_θ είναι η εφαρμογή μιας περιστροφής κατά γωνία θ γύρω από τον άξονα Z. Αυτό σημαίνει ότι αλλάζει τη φάση ενός qubit χωρίς να αλλάζει την πιθανότητα να βρεθεί στην κατάσταση |0⟩ ή |1⟩.

- Πύλη NOT :

$$NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Είναι η κβαντική αντίστοιχη της κλασικής πύλης NOT. Αναστρέφει την κατάσταση ενός qubit, μετατρέποντας το |0⟩ σε |1⟩ και το |1⟩ σε |0⟩.

- Πύλη Y :

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

Η λειτουργία της πύλης Y είναι να πραγματοποιήσει μια περιστροφή της κβαντικής κατάστασης ενός qubit γύρω από τον άξονα Y στον κβαντικό σφαιρικό αναπαραστατικό χώρο (Bloch sphere).

2.6.2 Κβαντικές πύλες πολλών qubit

- Πύλη CNOT :

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Είναι πύλη που εφαρμόζεται πάνω σε 2 qubit. Η πύλη CNOT περιλαμβάνει ένα control qubit και ένα target qubit. Η λειτουργία της εξαρτάται από την κατάσταση του control qubit. Αν το control qubit βρίσκεται στην κατάσταση |1⟩, τότε εφαρμόζεται η λειτουργία NOT στο target qubit. Αν το control qubit βρίσκεται στην κατάσταση |0⟩, τότε το target qubit παραμένει αμετάβλητο. Για παράδειγμα:

$$|00\rangle \rightarrow |00\rangle, \qquad |01\rangle \rightarrow |01\rangle$$
$$|10\rangle \rightarrow |11\rangle, \qquad |11\rangle \rightarrow |10\rangle$$

- Πύλη CZ (Controlled-Z):

$$CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

Όπως και η πύλη CNOT, η CZ έχει δύο qubit: ένα control qubit και ένα target qubit. Η λειτουργία της πύλης CZ εξαρτάται από την κατάσταση του control qubit. Αν το control qubit βρίσκεται στην κατάσταση |1⟩, τότε εφαρμόζεται η λειτουργία της πύλης Z στο target qubit. Αν το control qubit βρίσκεται στην κατάσταση |0⟩, τότε το target qubit παραμένει αμετάβλητο. Αν, δηλαδή, το control qubit βρίσκεται στην κατάσταση |1⟩, η πύλη CZ αλλάζει τη φάση του target qubit σε -1 χωρίς να αλλάζει την πιθανότητα της κατάστασης του qubit.

- Πύλη CU (Controlled-U):

$$CU = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U_{00} & U_{01} \\ 0 & 0 & U_{10} & U_{11} \end{pmatrix}$$

Με άλλα λόγια, η CU είναι μια πύλη δύο qubit που εφαρμόζει μια συγκεκριμένη λειτουργία (την πύλη U) στο target qubit, αλλά μόνο όταν το control qubit βρίσκεται σε μια συγκεκριμένη κατάσταση. Αν το control qubit βρίσκεται στην κατάσταση |1⟩, τότε η πύλη U εφαρμόζεται στο target qubit. Αν το control qubit βρίσκεται στην κατάσταση |0⟩, τότε το target qubit παραμένει αμετάβλητο.

- Πύλη SWAP:

$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Η πύλη SWAP εφαρμόζεται κι αυτή σε δύο qubits. Όπως υποδηλώνει το όνομά της, η κύρια λειτουργία της πύλης SWAP είναι να ανταλλάσσει τις καταστάσεις αυτών των δύο qubits. Αν έχουμε δύο qubits, A και B, και το A βρίσκεται στην κατάσταση |ψ⟩ και το B στην κατάσταση |φ⟩, η εφαρμογή της πύλης SWAP θα οδηγήσει στο A να βρίσκεται στην κατάσταση |φ⟩ και το B στην κατάσταση |ψ⟩.

- Πύλη Toffoli (CCNOT):

$$CCNOT = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

  Η πύλη Toffoli, επίσης γνωστή ως πύλη CCNOT (Controlled-Controlled NOT), λειτουργεί σε τρία qubit. Η πύλη Toffoli εφαρμόζει τη λειτουργία NOT στο τρίτο qubit (target) μόνο όταν τα πρώτα δύο qubit (control) βρίσκονται στην κατάσταση $|1\rangle$. Αν ένα ή και τα control qubit βρίσκονται στην κατάσταση $|0\rangle$, το target qubit δεν αλλάζει.

- Πύλη μέτρησης:
  Η πύλη μέτρησης παίρνει ένα qubit σε υπέρθεση σαν είσοδο και στην έξοδο εμφανίζει είτε 0 είτε 1. Μετρώντας ένα qubit, που η κβαντική του κατάσταση αναπαρίσταται από το διάνυσμα
  $\alpha|0\rangle + b|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$, θα δώσει αποτέλεσμα $|0\rangle$ με πιθανότητα $|\alpha|^2$ και $|1\rangle$ με πιθανότητα $|b|^2$.

2.7. Κβαντικά κυκλώματα

Στον κλασικό υπολογισμό, υπάρχουν τα λογικά κυκλώματα: αυτά αποτελούνται από μια περιορισμένη σειρά πυλών, και η έξοδός τους παρέχει το αποτέλεσμα ενός υπολογισμού. Στους κβαντικούς υπολογισμούς αντίστοιχα πρέπει να ορίσουμε ένα διαφορετικό μοντέλο υπολογισμών, το μοντέλο των κβαντικών κυκλωμάτων.

Ένα κβαντικό κύκλωμα μας δίνει τη δυνατότητα να περιγράψουμε μια σειρά από διαδοχικούς ορθομοναδιαίους μετασχηματισμούς που εφαρμόζονται στα qubits εισόδου. Ωστόσο, δεν μας επιτρέπει να απεικονίσουμε τη διαδικασία της μέτρησης, η οποία υποτίθεται ότι λαμβάνει χώρα στο τέλος του κυκλώματος, δηλαδή στο αποτέλεσμα των υπολογισμών.

Το σύνολο ενός κβαντικού κυκλώματος έχει ίδιο αριθμό εισόδων και εξόδων, κάτι που οφείλεται στο ότι το κύκλωμα, αφού δεν περιλαμβάνει διαδικασίες μέτρησης, αποτελεί έναν ορθομοναδιαίο μετασχηματισμό. Έτσι, κάθε κβαντικό κύκλωμα λειτουργεί αμφίδρομα, δηλαδή μπορεί να δουλέψει προς και από κάθε κατεύθυνση.

Στα κβαντικά κυκλώματα δεν είναι εφικτή η χρήση 'διακλαδώσεων'. Αυτό σημαίνει ότι εάν ένα κβαντικό bit χρησιμοποιείται ως είσοδος σε μία πύλη, τότε δεν μπορεί να χρησιμοποιηθεί παράλληλα στην είσοδο κάποιας άλλης πύλης ή ακόμα και σε διαφορετική είσοδο της ίδιας πύλης. Αυτός ο περιορισμός πηγάζει από την αρχή της αντιστρεψιμότητας στα κβαντικά συστήματα.

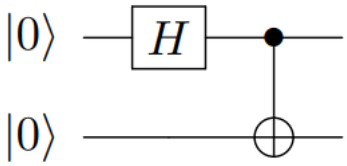
2.8. Καταστάσεις Bell

Οι καταστάσεις Bell αποτελούν ένα πολύ σημαντικό στοιχείο στον κβαντικό υπολογισμό και την κβαντική πληροφορική. Ονομάζονται αλλιώς καταστάσεις μέγιστης συμπλοκής. Υπάρχουν τέσσερις καταστάσεις Bell, οι οποίες ορίζονται ως εξής:

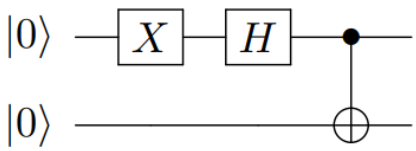
$|\psi^+\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ (1) $|\psi^-\rangle = \frac{|00\rangle-|11\rangle}{\sqrt{2}}$ (2) $|\varphi^+\rangle = \frac{|01\rangle+|10\rangle}{\sqrt{2}}$ (3) $|\varphi^-\rangle = \frac{|01\rangle-|10\rangle}{\sqrt{2}}$ (4)

Οι παραπάνω καταστάσεις κατασκευάζονται από τα παραπάκτω κυκλώματα:

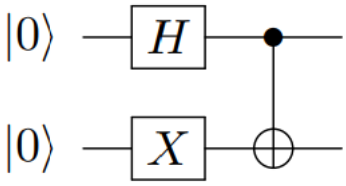
(1):

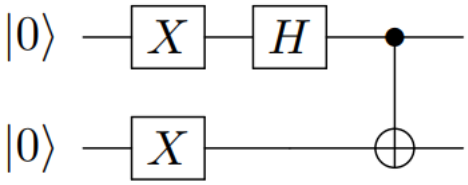


(2):



(3):





2.9. No-Cloning theorem

Θεώρημα: Δεν είναι δυνατή η δημιουργία ενός ακριβούς και πιστού αντιγράφου μιας άγνωστης κβαντικής κατάστασης.

Αυτό σημαίνει ότι, σε αντίθεση με τις κλασικές πληροφορίες που μπορούν να αντιγραφούν ελεύθερα, ένα κβαντικό σύστημα δεν μπορεί να αντιγραφεί χωρίς να διαταραχθεί η αρχική κατάσταση. Το θεώρημα απορρέει από την γραμμικότητα της κβαντικής μηχανικής και την αδυναμία διάκρισης μη ορθογώνιων καταστάσεων. Η διαδικασία της μέτρησης στην κβαντική μηχανική είναι επίσης ένας παράγοντας που συμβάλλει στην αδυναμία του κλωνισμού.

2.10. Προκλήσεις Κβαντικών Υπολογιστών

Ο θόρυβος αποτελεί μία από τις σημαντικότερες προκλήσεις του κβαντικού υπολογισμού, κυρίως επειδή η θερμότητα μπορεί να επηρεάσει σημαντικά την απόδοση και την αξιοπιστία των qubits, τα οποία είναι τα βασικά στοιχεία των κβαντικών υπολογιστών. Η θερμότητα προκαλεί θερμικές διακυμάνσεις που μπορούν να διαταράξουν τις κβαντικές καταστάσεις των qubits. Αυτές οι διαταραχές μπορούν να προκαλέσουν απώλεια πληροφορίας και λάθη στους υπολογισμούς. Η διαχείριση της θερμότητας είναι ζωτικής σημασίας για την αποδοτική λειτουργία των κβαντικών υπολογιστών. Μέσω της χρήσης κρυογονικής τεχνολογίας και της συνεχούς βελτίωσης των υλικών και των τεχνολογιών, οι ερευνητές επιδιώκουν να μειώσουν τον αντίκτυπο της θερμότητας και να βελτιώσουν την απόδοση και την αξιοπιστία των κβαντικών υπολογιστών.

2.11 Noisy Intermediate Scale Quantum

Στη φάση αυτή, βρισκόμαστε ανάμεσα στα πρώτα πειραματικά κβαντικά συστήματα και τους πλήρως λειτουργικούς κβαντικούς υπολογιστές του μέλλοντος, οι οποίοι θα έχουν τη δυνατότητα να εκτελούν υπολογισμούς που δεν είναι δυνατοί με τους σημερινούς κλασικούς υπολογιστές. Οι NISQ συσκευές διαθέτουν μεταξύ 50 και κάποιων εκατοντάδων qubits. Αυτό επιτρέπει την εκτέλεση πειραμάτων και αλγορίθμων που δεν μπορούν να εκτελεστούν από τους κλασικούς υπολογιστές, αλλά είναι ακόμα μακριά από την επίτευξη του πλήρους δυναμικού της κβαντικής υπολογιστικής. Οι NISQ υποφέρουν από σημαντικό επίπεδο κβαντικού θορύβου, ο οποίος δυσχεραίνει την ακριβή εκτέλεση κβαντικών αλγορίθμων.

2.12 Error correction στους Κβαντικούς Υπολογιστές

Η διόρθωση λαθών στους κβαντικούς υπολογιστές είναι μια κρίσιμη πτυχή της κβαντικής υπολογιστικής, που επιτρέπει την ακριβή εκτέλεση υπολογισμών παρά την παρουσία θορύβου και άλλων διαταρακτικών επιδράσεων που μπορούν να προκαλέσουν λάθη στα qubits. Ένας κβαντικός υπολογιστής πλήρους κλίμακας απαιτεί διόρθωση λαθών. Η διόρθωση καθών απαιτεί αυξημένους πόρους για την υλοποίηση της. Απαιτεί σημαντικά περισσότερα qubits και υπολογιστική ισχύ για την εφαρμογή των αλγορίθμων διόρθωσης. Η επίτευξη αποτελεσματικής διόρθωσης λαθών είναι θεμελιώδης για την ανάπτυξη κβαντικών υπολογιστών και αποτελεί ενεργό πεδίο έρευνας στην κβαντική υπολογιστική.

3. Παραγωγή Ψευδοτυχαίων Ακολουθιών

Στη σύγχρονη εποχή της τεχνολογικής εξέλιξης, η κβαντική υπολογιστική αναδεικνύεται ως ένας τομέας πρωτοποριακής σημασίας, ανοίγοντας νέους δρόμους στην επεξεργασία πληροφοριών και στην αλγοριθμική επίλυση προβλημάτων. Ένα σημαντικό πεδίο εφαρμογής της κβαντικής υπολογιστικής είναι η παραγωγή ψευδοτυχαίων ακολουθιών, μια διαδικασία κεντρικής σημασίας για πολλές εφαρμογές, από την κρυπτογράφηση μέχρι τη στατιστική ανάλυση. Η κβαντική εκδοχή των κλασικών μεθόδων παραγωγής τυχαίων ακολουθιών, όπως οι Linear Feedback Shift Register Generators, ανοίγει πρωτοποριακές δυνατότητες για την αύξηση της απόδοσης και της ασφάλειας σε αυτό το πεδίο, παρέχοντας μια νέα προοπτική στην έρευνα και την ανάπτυξη προηγμένων τεχνολογικών λύσεων. Σε αυτή την εργασία,η υλοποίηση της κβαντικής έκδοσης αυτή της μεθόδου είναι η κεντρική ιδέα. Ας δούμε όμως πρώτα πως την κεντρική ιδέα γύρω από τις LFSR γεννήτριες στην κλασσική υπολογιστική.

3.1. Linear Feedback Shift Register

Οι LFSR είναι συστήματα που χρησιμοποιούνται για την παραγωγή ψευδοτυχαίων ακολουθιών αριθμών. Αυτές οι ακολουθίες φαίνονται τυχαίες, αλλά δημιουργούνται από μια σταθερή, επαναλαμβανόμενη διαδικασία. Τα LFSR χρησιμοποιούνται στην κρυπτογραφία, στις τηλεπικοινωνίες, και στην επεξεργασία ψηφιακών σημάτων. Στις γεννήτριες LFSR το εισαγόμενο bit είναι μια γραμμική συνάρτηση της προηγούμενης κατάστασής του. Μία γεννήτρια LFSR είναι συνήθως ένας μετατοπιστής του οποίου το εισαγόμενο bit καθοδηγείται από το XOR κάποιων bits της συνολικής τιμής του μετατοπιστή.

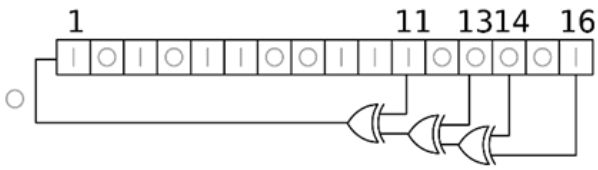
Το αρχικό σημείο εκκίνησης μιας γεννήτριας LFSR αποκαλείται σπόρος (seed). Λόγω της ντετερμινιστικής φύσης του LFSR, η σειρά των τιμών που παράγει εξαρτάται πλήρως από την τρέχουσα (ή προηγούμενη) κατάστασή του. Επειδή η γεννήτρια LFSR έχει περιορισμένο αριθμό ενδεχόμενων καταστάσεων, αναπόφευκτα θα επαναλάβει τις τιμές του σε έναν κύκλο. Ωστόσο, μια γεννήτρια LFSR με μια κατάλληλα επιλεγμένη συνάρτηση ανατροφοδότησης είναι ικανή να δημιουργήσει μια σειρά από bits που μοιάζουν τυχαία και έχουν έναν πολύ μακρύ κύκλο. Η μαθηματική θεμελίωση των LFSR τις καθιστά ιδιαίτερα ενδιαφέρουσες για μελέτη και εφαρμογή. Με τη χρήση βασικών στοιχείων, κάποιος μπορεί να δημιουργήσει σχετικά περίπλοκες λογικές δομές.

3.2. Πολυώνυμο Ανατροφοδότησης

Το πολυώνυμο ανατροφοδότησης είναι αυτό που ορίζει την αρχιτεκτονική και τον τρόπο λειτουργίας ενός LFSR. Η διαδικασία "ανατροφοδότησης" εξαρτάται από την τεχνική με την οποία τα bits της τρέχουσας κατάσταση συνδυάζονται γραμμικά (μέσω της εφαρμογής των λειτουργιών XOR) για τη δημιουργία ενός νέου bit σε κάθε επανάληψη της διαδικασίας μετατόπισης. Η επεξεργασία των bits με βάση το πολυώνυμο ανατροφοδότησης γίνεται χρησιμοποιώντας την αριθμητική modulo-2, αντανακλώντας τη χρήση του όρου "γραμμικό" στην ονομασία LFSR. Σε αυτό το πλαίσιο, η πράξη της πρόσθεσης (+) αντιστοιχεί στη λειτουργία XOR ενώ η πράξη του πολλαπλασιασμού (×) αντανακλά τη λειτουργία AND.

3.3. Fibonacci LFSRs

Οι θέσεις των bits σε μία γεννήτρια LFSR που επιδρούν στην επόμενη κατάσταση της γεννήτριας αποκαλούνται "απολήξεις" (taps). Στο παράδειγμα παρακάτω, αυτές οι απολήξεις είναι [16,14,13,11]. Το bit στην πιο δεξιά θέση του LFSR ονομάζεται το εξαγόμενο bit και είναι επίσης μια από τις απολήξεις. Αυτές οι απολήξεις συνδέονται μεταξύ τους μέσω της λειτουργίας XOR διαδοχικά και στη συνέχεια το αποτέλεσμα επανεισάγεται στο αριστερότερο bit. Η σειρά των bits που παράγεται από τη δεξιότερη θέση ονομάζεται η εξαγόμενη ακολουθία (output stream).



Παράδειγμα: Ένας 16-bit Fibonacci LFSR. Πολυώνυμο ανάδρασης $x^{16} + x^{14} + x^{13} + x^{11} + 1$

Παράδειγμα σε C

```c
#include <stdint.h>
unsigned lfsr_fib(void)
{
    uint16_t start_state = 0xACE1u;  /* Any nonzero start state will work. */
    uint16_t lfsr = start_state;
    uint16_t bit;                    /* Must be 16-bit to allow bit<<15 later in the code
*/  unsigned period = 0;

    do
    {   /* taps: 16 14 13 11; feedback polynomial: x^16 + x^14 + x^13 + x^11 + 1 */
        bit = ((lfsr >> 0) ^ (lfsr >> 2) ^ (lfsr >> 3) ^ (lfsr >> 5)) & 1u;
        lfsr = (lfsr >> 1) | (bit << 15);
        ++period;
    }
    while (lfsr != start_state);

    return period;
}
```

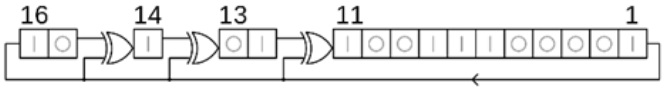
Παράδειγμα σε Python

```
start_state = 1 << 15 | 1
lfsr = start_state
period = 0

while True:
    #taps: 16 15 13 4; feedback polynomial: x^16 + x^14 + x^13 + x^11 + 1
    bit = (lfsr ^ (lfsr >> 2) ^ (lfsr >> 3) ^ (lfsr >> 5)) & 1
    lfsr = (lfsr >> 1) | (bit << 15)
    period += 1
    if (lfsr == start_state):
        print(period)
        break
```

3.4 Galois LFSRs

Αυτή η δομή μπορεί να παράγει την ίδια ακολουθία εξόδου όπως ένας κλασικός LFSR, αλλά με κάποια χρονική καθυστέρηση. Στο Galois LFSR, τα bits που δεν αποτελούν απολήξεις μετατοπίζονται δεξιά χωρίς να αλλάζουν όταν το σύστημα ενεργοποιείται, ενώ τα bits των απολήξεων συνδυάζονται με XOR με το εξαγόμενο bit πριν μετατοπιστούν στην επόμενη θέση. Το νέο εξαγόμενο bit γίνεται το επόμενο εισαγόμενο bit. Έτσι, όταν το εξαγόμενο bit είναι μηδέν, όλα τα bits μετατοπίζονται δεξιά χωρίς να αλλάζουν και το εισαγόμενο bit γίνεται επίσης μηδέν. Αντίθετα, όταν το εξαγόμενο bit είναι ένα, τα bits στις θέσεις των απολήξεων αντιστρέφονται (τα 0 γίνονται 1 και τα 1 γίνονται 0), και ολόκληρος ο μετατοπιστής μετατοπίζεται δεξιά με το εισαγόμενο bit να γίνεται 1.



Ένας 16-bit Galois LFSR. Οι αριθμοί των καταχωρητών που αναγράφονται παραπάνω αντιστοιχούν στο ίδιο πρωτόγονο πολυώνυμο με το παράδειγμα Fibonacci, αλλά μετριούνται αντίστροφα προς την κατεύθυνση της μετατόπισης

Για την παραγωγή της ίδιας εξαγόμενης ακολουθίας σε έναν LFSR Galois, η σειρά των απολήξεων πρέπει να είναι αντίστροφη σε σχέση με αυτή σε έναν συμβατικό LFSR, αλλιώς η παραγόμενη ακολουθία θα είναι αντίστροφη. Είναι σημαντικό να σημειωθεί ότι η εσωτερική κατάσταση του LFSR μπορεί να μην είναι ίδια. Ο καταχωρητής Galois που περιγράφεται εδώ δημιουργεί την ίδια εξαγόμενη ακολουθία με έναν καταχωρητή Fibonacci, όπως αναφέρεται στην πρώτη ενότητα, αλλά με μια χρονική διαφορά, που σημαίνει ότι απαιτείται διαφορετικό σημείο εκκίνησης για την παραγωγή της ίδιας εξόδου σε κάθε κύκλο.

Στους LFSR Galois, δεν γίνεται συνδυασμός όλων των απολήξεων για την παραγωγή του νέου εισαγόμενου bit (καθώς η λειτουργία XOR εκτελείται εσωτερικά και δεν απαιτούνται πολλαπλές πύλες XOR σε αλληλουχία, μειώνοντας έτσι τους χρόνους διάδοσης σε αυτούς ενός μόνο XOR). Αυτό επιτρέπει τον παράλληλο υπολογισμό για κάθε απόληξη, αυξάνοντας την ταχύτητα εκτέλεσης του LFSR.

Παράγειγμα σε C

```c
#include <stdint.h>
unsigned lfsr_galois(void)
{
    uint16_t start_state = 0xACE1u;  /* Any nonzero start state will work. */
    uint16_t lfsr = start_state;
    unsigned period = 0;

    do
    {
#ifndef LEFT
        unsigned lsb = lfsr & 1u;  /* Get LSB (i.e., the output bit). */
        lfsr >>= 1;                /* Shift register */
        if (lsb)                   /* If the output bit is 1, */
            lfsr ^= 0xB400u;       /*  apply toggle mask. */
#else
        unsigned msb = (int16_t) lfsr < 0;   /* Get MSB (i.e., the output bit). */
        lfsr <<= 1;                          /* Shift register */
        if (msb)                             /* If the output bit is 1, */
            lfsr ^= 0x002Du;                 /*  apply toggle mask. */
#endif
        ++period;
    }
    while (lfsr != start_state);

    return period;
}
```

Παράδειγμα σε Python

```python
def lfsr_galois():
    start_state = 0xACE1  # Οποιαδήποτε μη μηδενική αρχική κατάσταση θα λειτουργήσει.
    lfsr = start_state
    period = 0

    while True:
        lsb = lfsr & 1  # Λήψη LSB (δηλαδή του εξερχόμενου bit).
        lfsr >>= 1  # Μετατόπιση του μητρώου
        if lsb:  # Αν το εξερχόμενο bit είναι 1,
            lfsr ^= 0xB400  # εφαρμόζεται το toggle mask.

        period += 1
        if lfsr == start_state:
            break

    return period

# Εκτέλεση της συνάρτησης
period = lfsr_galois()
print(f"Περίοδος: {period}")
```

3.5 Xorshift LFSRs

Οι Xorshift LFSRs χρησιμοποιούν τις λειτουργίες XOR και Shift (Μετατόπιση). Αυτή η τεχνική είναι ιδιαιτέρως αποτελεσματική για γρήγορη υλοποίηση σε λογισμικό, καθώς αυτές οι λειτουργίες μπορούν να αντιστοιχιστούν αποδοτικά με τις εντολές των σύγχρονων επεξεργαστών.

Η λειτουργία XOR χρησιμοποιείται για να εφαρμόσει την ανατροφοδότηση στον LFSR, επηρεάζοντας τα επιλεγμένα bits (σημεία απόληξης) για τη δημιουργία της επόμενης κατάστασης του μετατοπιστή. Η λειτουργία Shift, από την άλλη, είναι υπεύθυνη για τη μετακίνηση των bits εντός του μετατοπιστή είτε προς τα δεξιά είτε προς τα αριστερά, ανάλογα με τον τρόπο υλοποίησης του LFSR.

Η ευκολία με την οποία μπορούν να εκτελεστούν αυτές οι εντολές σε σύγχρονους επεξεργαστές καθιστά τους Xorshift LFSRs ιδιαίτερα χρήσιμους για εφαρμογές που απαιτούν γρήγορες λειτουργίες, όπως η παραγωγή ψευδοτυχαίων αριθμών, η κρυπτογράφηση δεδομένων, και η δημιουργία δοκιμαστικών ακολουθιών για τεστάρισμα και προσομοίωση.

Υλοποίηση σε C

```c
#include <stdint.h>
unsigned lfsr_xorshift(void)
{
    uint16_t start_state = 0xACE1u;  /* Any nonzero start state will work. */
    uint16_t lfsr = start_state;
    unsigned period = 0;

    do
    {   // 7,9,13 triplet from http://www.retroprogramming.com/2017/07/xorshift-pseudorandom-numbers-in-z80.html
        lfsr ^= lfsr >> 7;
        lfsr ^= lfsr << 9;
        lfsr ^= lfsr >> 13;
        ++period;
    }
    while (lfsr != start_state);

    return period;
}
```

Υλοποίηση σε python

```python
def lfsr_xorshift():
    start_state = 0xACE1  # Αρχική κατάσταση
    lfsr = start_state
    period = 0

    while True:
        # Εκτέλεση των βημάτων XOR μετατόπισης
        lfsr ^= (lfsr >> 7)
        lfsr ^= (lfsr << 9)
        lfsr ^= (lfsr >> 13)
        period += 1

        if lfsr == start_state:
            break

    return period

# Εκτέλεση της συνάρτησης
period = lfsr_xorshift()
print("Περίοδος:", period)
```

3.6 Matrix forms

Οι Δυαδικοί Γραμμικοί Ανατροφοδοτούμενοι Μετατοπιστές (LFSRs) μπορούν να παρουσιαστούν και να λειτουργήσουν ως πίνακες, πράγμα που αποδεικνύεται ιδιαίτερα ωφέλιμο τόσο στην εξέταση όσο και στον σχεδιασμό τους, αλλά και στην υλοποίησή τους σε πιο σύνθετες εφαρμογές όπως η κρυπτογραφία και η θεωρία των κωδικών.

Κάθε LFSR μπορεί να εκφραστεί μέσω ενός πίνακα με διαστάσεις n x n για ένα n-bit LFSR, όπου οι στήλες αντικατοπτρίζουν την κατάσταση κάθε bit. Οι ενέργειες μετατόπισης και XOR στο πλαίσιο ενός LFSR μπορούν να απεικονιστούν μέσω πράξεων πολλαπλασιασμού και πρόσθεσης πινάκων, με τη μετατόπιση προς τα δεξιά να αντιστοιχεί σε καθοδική μετακίνηση των γραμμών του πίνακα. Οι θέσεις των taps και το σχετικό πολυώνυμο ανατροφοδότησης επίσης παρουσιάζονται ως πίνακας, κρίσιμο για την κατανόηση της δομής και λειτουργίας του LFSR.

Ο πίνακας που αντιστοιχεί σε έναν Γραμμικό-Ανατροφοδοτούμενο Μετατοπιστή (Linear Feedback Shift Register - LFSR) Fibonacci:

$$\begin{pmatrix} a_k \\ a_{k+1} \\ a_{k+2} \\ \vdots \\ a_{k+n-1} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ c_0 & c_1 & \cdots & \cdots & c_{n-1} \end{pmatrix} \begin{pmatrix} a_{k-1} \\ a_k \\ a_{k+1} \\ \vdots \\ a_{k+n-2} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ c_0 & c_1 & \cdots & \cdots & c_{n-1} \end{pmatrix}^k \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1} \end{pmatrix}$$

Ο πίνακας που αντιστοιχεί σε έναν Γραμμικό-Ανατροφοδοτούμενο Μετατοπιστή (Linear Feedback Shift Register - LFSR) σε διαμόρφωση Galois:

$$\begin{pmatrix} c_0 & 1 & 0 & \cdots & 0 \\ c_1 & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ c_{n-2} & 0 & \cdots & 0 & 1 \\ c_{n-1} & 0 & \cdots & \cdots & 0 \end{pmatrix}^k \begin{pmatrix} a'_0 \\ a'_1 \\ a'_2 \\ \vdots \\ a'_{n-1} \end{pmatrix}$$

3.7 Εναλλακτική υλοποίηση LFSR

Ως εναλλακτική στην αντίστροφη συνάρτηση XOR που χρησιμοποιείται σε έναν LFSR, μπορεί κανείς να χρησιμοποιήσει την XNOR που οδηγεί σε έναν ισοδύναμο πολυωνυμικό μετρητή του οποίου η κατάσταση είναι το συμπλήρωμα της κατάστασης ενός LFSR. Μια κατάσταση με όλα

τα bits στην τιμή ένα δεν είναι «αποδεκτή» όταν χρησιμοποιείται αντίστροφη συνάρτηση XNOR, όπως και μια κατάσταση με όλα τα bits στο μηδέν δεν είναι «αποδεκτή» με τη χρήση XOR. Αυτή η κατάσταση θεωρείται μη αποδεκτή επειδή ο μετρητής θα παρέμενε "κλειδωμένος" σε αυτή. Αυτή η μέθοδος μπορεί να είναι πλεονεκτική σε υλικούς LFSR που χρησιμοποιούν flip-flops και ξεκινούν σε μηδενική κατάσταση, καθώς δεν ξεκινούν σε κατάσταση κλειδώματος, πράγμα που σημαίνει ότι ο μετατοπιστής δεν χρειάζεται να λάβει αρχική τιμή για να ξεκινήσει τη λειτουργία του.

3.8 Πολυώνυμο μεγίστου μήκους

Ένας LFSR μεγίστου μήκους δημιουργεί μια ακολουθία m (m-sequence), η οποία περιλαμβάνει όλες τις δυνατές $2^m - 1$ καταστάσεις μέσα στον LFSR, εκτός από την κατάσταση όπου όλα τα bits είναι μηδενικά. Αν ο LFSR βρίσκεται σε μια κατάσταση όπου όλα τα bits είναι μηδενικά, τότε δεν θα είναι δυνατή η αλλαγή της κατάστασής του.

Τα πολυώνυμα μεγίστου μήκους, γνωστά και ως πολυώνυμα M-Sequence, είναι κρίσιμης σημασίας στην κατασκευή γεννητριών Linear Feedback Shift Register (LFSR). Αυτά τα πολυώνυμα χρησιμοποιούνται για την επίτευξη της μέγιστης περιόδου ακολουθιών που μπορούν να παραχθούν από ένα LFSR, προσφέροντας εξαιρετική επίδοση σε εφαρμογές όπως η κρυπτογραφία, οι ψευδοτυχαίες ακολουθίες και η δοκιμή κυκλωμάτων.

3.9 LFSR και Γραμμική Πολυπλοκότητα

Η γραμμική πολυπλοκότητα L(s) μιας άπειρης δυαδικής ακολουθίας s=$\{s_j\}_j$ με τον εξής τρόπο:

- αν το s είναι μία μηδενική ακολουθία, τότε L(s)=0
- αν δεν υπάρχει κανένα LFSR που να παράγει το s,τότε L(s)=∞
- αν το s μπορεί να παραχθεί από έναν ή περισσότερους LFSR, τότε L(s) αντιστοιχεί στο μήκος του μικρότερου LFSR που μπορεί να το παράγει. Αντίστοιχα, L(s) αντιπροσωπεύει τον βαθμό του ελάχιστου πολυωνύμου του s.

Αν S_n είναι μια πεπερασμένη δυαδική ακολουθία, τότε $L(S_n)$ είναι το μήκος του συντομότερου LFSR το οποίο έχει ως πρώτους n όρους το S_n. Η γραμμική πολυπλοκότητα ικανοποιεί τις ακόλουθες ιδιότητες:

Θεωρούμε S_n δυαδική ακολουθία τότε

1. $0 \leq L(S_n) \leq n$ *όπου* $n \geq 1$
2. $L(S_n) = 0$ *αν και μόνο αν* S_n *είναι μηδενική ακολουθία με μήκος* n

3. $L(S_n) = n$ *αν και μόνο αν* $S_n = 0,0,\ldots,01$
4. *Αν* S_n *είναι περιοδική με περίοδο* T *τότε* $L(S_n) \leq T$
5. H *L ικανοποιεί ανισότητα τριγώνου, δηλαδή* $L(s \oplus t) \leq L(s) + L(t)$ *όπου* $s \oplus t$, *δυαδική* xor *των* s, t
6. *Αν το πολυώνυμο ανατροφοδότησης* $f(x)$ *είναι πρωτόγονο πάνω στο* $F2[x]$, *τότε κάθε μία από τις* $2n - 1$ *μη μηδενικές καταστάσεις του συναφούς μη μοναδικού LFSR* $L(S_n) = n$
7. *Αν το πολυώνυμο ανατροφοδότησης f(x) έχει βαθμό n και είναι ανάγωγο πάνω στο F2[x], με α ρίζα του f(x) στο F2n, τότε η περίοδος του LFSR είναι ίση με την τάξη του α στο F2n. Κατά συνέπεια, η περίοδος ενός LFSR με n στάδια πάντα διαιρεί το 2n−1.*

3.10 Ιδιότητες Εξαγόμενης Ακολουθίας

- **Εμφάνιση 0 και 1 σε σειρές:** Στην ακολουθία που προκύπτει, τα μηδενικά και οι μονάδες δημιουργούν συνεχόμενες ομάδες. Παίρνοντας για παράδειγμα την ακολουθία 1110010, αυτή διαρθρώνεται σε τέσσερις ομάδες με διάρκειες 3, 2, 1, και 1 αντιστοίχως. Κατά τη διάρκεια μιας πλήρους περιόδου ενός LFSR με το μέγιστο δυνατό μήκος, συναντώνται 2^n−1 τέτοιες ομάδες (σύμφωνα με το παράδειγμα, ένας LFSR 3-bit περιλαμβάνει 4 ομάδες). Ακριβώς το ήμισυ από αυτές τις ομάδες έχει μήκος ενός bit, το ένα τέταρτο δύο bits, ενώ υπάρχει μόνο μία ομάδα μηδενικών με μήκος n − 1 bits και μία ομάδα μονάδων με μήκος n bits. Η κατανομή αυτή είναι σχεδόν ίδια με την κατανομή που θα περιμέναμε στατιστικά από μια πραγματικά τυχαία ακολουθία, παρόλο που η πιθανότητα να εμφανιστεί ακριβώς αυτή η κατανομή σε ένα δείγμα πραγματικά τυχαίας ακολουθίας είναι σχετικά χαμηλή.
- **Η Εξαγόμενη Ακολουθία είναι Ντετερμινιστική:** Όταν είναι γνωστή η τρέχουσα κατάσταση και οι θέσεις των πυλών XOR ενός LFSR, μπορούμε να προβλέψουμε τι θα συμβεί στο επόμενο βήμα. Αυτή η δυνατότητα πρόβλεψης διαφέρει από την απόλυτη αβεβαιότητα που χαρακτηρίζει τα πραγματικά τυχαία συμβάντα. Στην περίπτωση των LFSR με την μέγιστη δυνατή εκτελεσιμότητα, η πρόβλεψη της αμέσως επόμενης κατάστασης γίνεται ακόμα πιο απλή, δεδομένου ότι για κάθε δεδομένο μήκος υπάρχει μόνο ένας περιορισμένος αριθμός δυνατών καταστάσεων.
- **Η Εξαγόμενη Ακολουθία είναι Αντιστρέψιμη:** Ένας LFSR με αντικατοπτρισμένες απολήξεις θα διανύσει την εξαγόμενη ακολουθία σε αντίστροφη σειρά.
- **Η Τιμή που Αποτελείται Μόνο από Μηδενικά Δεν Μπορεί να Εμφανιστεί:** Έτσι, ένας LFSR μήκους n δεν μπορεί να χρησιμοποιηθεί για να παράγει όλες τις τιμές 2^n

4. Κβαντική έκδοση της γεννήτριας LFSR

4.1. Κβαντικοί προσομοιωτές

Οι quantum simulators ή κβαντικοί προσομοιωτές είναι συστήματα που χρησιμοποιούνται για τη μοντελοποίηση και την προσομοίωση των κβαντικών φαινομένων, προσφέροντας μια προσέγγιση στον τρόπο λειτουργίας των κβαντικών υπολογιστών. Αυτός ο τύπος τεχνολογίας παρέχει σημαντικές δυνατότητες για την έρευνα και την ανάπτυξη στον τομέα της κβαντικής υπολογιστικής, επιτρέποντας την προσομοίωση συστημάτων που είναι πολύ περίπλοκα για να μοντελοποιηθούν με τους κλασικούς υπολογιστές.

Οι κβαντικοί προσομοιωτές επιτρέπουν την ανάπτυξη, την προσομοίωση και τη δοκιμή κβαντικών αλγορίθμων πριν αυτοί εκτελεστούν σε πραγματικούς κβαντικούς υπολογιστές. Λειτουργούν ως πολύτιμα εκπαιδευτικά εργαλεία για την κατανόηση της κβαντικής υπολογιστικής και της κβαντικής μηχανικής. Πολλοί κβαντικοί προσομοιωτές είναι διαθέσιμοι μέσω cloud πλατφορμών, επιτρέποντας την εύκολη πρόσβαση και χρήση από ερευνητές και αναπτυξιακές ομάδες παγκοσμίως. Δύο από τις πιο γνωστές πλατφόρμες που προσφέρουν πρόσβαση σε κβαντικούς προσομοιωτές είναι η IBM Quantum Experience και η Google Quantum AI.

4.2. IBM Quantum Experience

Η πλατφόρμα IBM Quantum Experience είναι ένας πρωτοποριακός cloud service που παρέχει πρόσβαση σε κβαντικούς υπολογιστές και σε εργαλεία για την ανάπτυξη και τεστάρισμα κβαντικών αλγορίθμων. Στοχεύει σε ερευνητές, επιστήμονες και ενδιαφερόμενους από τη βιομηχανία και την εκπαίδευση, προσφέροντας μια πρακτική προσέγγιση στην κβαντική υπολογιστική.

Η IBM παρέχει πρόσβαση σε διάφορους κβαντικούς υπολογιστές με διαφορετικό αριθμό κβαντικών bits (qubits), επιτρέποντας την εκτέλεση πειραμάτων και τον σχεδιασμό κβαντικών αλγορίθμων. Προσφέρει εργαλεία όπως το Qiskit, ένα open-source κβαντικό προγραμματιστικό πλαίσιο, το οποίο επιτρέπει την κατασκευή, την προσομοίωση και την εκτέλεση κβαντικών προγραμμάτων σε πραγματικούς κβαντικούς υπολογιστές.

4.3. Qiskit

Το Qiskit είναι ένα ανοιχτού κώδικα κβαντικό προγραμματιστικό πλαίσιο που αναπτύχθηκε από την IBM. Διαθέτει ευέλικτη αρχιτεκτονική και διαρθρώνεται σε τέσσερις βασικούς τομείς καθένας από τους οποίους εξυπηρετεί διαφορετικές ανάγκες στην κβαντική υπολογιστική.

- Terra: Παρέχει τα εργαλεία για το χαμηλού επιπέδου προγραμματισμό κβαντικών κυκλωμάτων, την προσομοίωση και την εκτέλεση σε πραγματικούς κβαντικούς υπολογιστές.

- Aer: Προσφέρει προσομοιωτές και εργαλεία για τη βελτιστοποίηση και τη δοκιμή κβαντικών αλγορίθμων και κυκλωμάτων σε κλασικούς υπολογιστές.

- Ignis: Αφορά την κβαντική μετρολογία, την ανίχνευση και την διόρθωση σφαλμάτων σε κβαντικά συστήματα. Η κβαντική μετρολογία είναι ένας τομέας που αφορά τη χρήση κβαντικών φαινομένων για την μέτρηση φυσικών μεγεθών με την υψηλότερη δυνατή ακρίβεια και ευαισθησία.

- Aqua: Παρέχει υψηλού επιπέδου αλγορίθμους. Εκεί υπάρχουν έτοιμοι, υλοποιημένοι αλγόριθμοι χωρισμένοι σε «πακέτα» ανάλογα το πεδίο (μηχανική μάθηση, χρηματοοικονομικά, χημεία κλπ) πάνω στο οποίο θέλουμε να αναπτύξουμε μια εφαρμογή που θα τρέχει σε κβαντικό υπολογιστή.

Οι χρήστες μπορούν να χρησιμοποιήσουν το Qiskit για να γράφουν κβαντικά προγράμματα σε Python, τα οποία στη συνέχεια μπορούν να προσομοιωθούν σε κλασικούς υπολογιστές ή να εκτελεστούν σε πραγματικούς κβαντικούς υπολογιστές μέσω της IBM Quantum Experience. Το Qiskit αποτελεί έναν ουσιαστικό πόρο για την κβαντική υπολογιστική κοινότητα, προσφέροντας μια πλατφόρμα για την εκπαίδευση, την έρευνα, και την ανάπτυξη κβαντικών τεχνολογιών. Με την ευκολία χρήσης και την ευρεία προσβασιμότητα, το Qiskit καθιστά δυνατή την εξερεύνηση και την αξιοποίηση της κβαντικής υπολογιστικής από ένα ευρύ φάσμα.

4.4. Google Quantum AI

Η Google Quantum AI είναι η πρωτοβουλία της Google στον τομέα της κβαντικής υπολογιστικής, επικεντρώνεται στην ανάπτυξη και την εφαρμογή κβαντικών τεχνολογιών για την επίλυση προβλημάτων που δεν είναι εφικτή με τους σημερινούς κλασικούς υπολογιστές. Η προσπάθεια αυτή συνδυάζει την ερευνητική δουλειά στον κβαντικό υπολογισμό με τις προηγμένες τεχνολογίες τεχνητής νοημοσύνης (AI) της Google, με στόχο την εξερεύνηση νέων τρόπων για την επιτάχυνση της επιστημονικής προόδου και την ανάπτυξη νέων τεχνολογικών εφαρμογών.

Ένα από τα πιο δημοφιλή επιτεύγματα της Google Quantum AI είναι η ανάπτυξη του κβαντικού υπολογιστή Sycamore. Το 2019, η Google ανακοίνωσε ότι ο Sycamore επέτυχε το λεγόμενο

"κβαντικό πλεονέκτημα", εκτελώντας μια ειδική υπολογιστική εργασία σε 200 δευτερόλεπτα, μια διαδικασία που θα απαιτούσε περίπου 10.000 χρόνια από τον πιο γρήγορο κλασικό υπερυπολογιστή της εποχής εκείνης. Εκτός από την επίτευξη κβαντικού πλεονεκτήματος, η Google Quantum AI ερευνά την εφαρμογή της κβαντικής υπολογιστικής σε τομείς όπως η κβαντική χημεία, η υλικοεπιστήμη, η τεχνητή νοημοσύνη και οι αλγοριθμικές προκλήσεις, με στόχο την επίλυση προβλημάτων που θα είχαν μεγάλο αντίκτυπο στην κοινωνία και την βιομηχανία.

4.5 Cirq

Η Cirq είναι ένα ανοιχτού κώδικα κβαντικό προγραμματιστικό πλαίσιο που αναπτύχθηκε από την Google, μέρος της πρωτοβουλίας της για την Quantum AI. Σχεδιάστηκε για την ανάπτυξη, τη δοκιμή και την προσομοίωση κβαντικών κυκλωμάτων σε επίπεδο κβαντικών bits (qubits). Η Cirq παρέχει μια διαύγεια για τον σχεδιασμό κβαντικών κυκλωμάτων, επιτρέποντας στους προγραμματιστές να δημιουργούν και να πειραματίζονται με κβαντικά προγράμματα που εκτελούνται σε κβαντικούς υπολογιστές. Είναι σχεδιασμένη να υποστηρίζει διάφορους τύπους κβαντικών υπολογιστών και προσομοιωτών, προσφέροντας επίσης τη δυνατότητα στους χρήστες να επεκτείνουν και να προσαρμόζουν το πλαίσιο σύμφωνα με τις συγκεκριμένες ανάγκες τους. Προσφέρει εργαλεία για την προσομοίωση κβαντικών κυκλωμάτων σε κλασικούς υπολογιστές, καθώς και διεπαφές για την εκτέλεση προγραμμάτων σε πραγματικούς κβαντικούς υπολογιστές, όπως οι κβαντικοί υπολογιστές που διατίθενται μέσω της πλατφόρμας Google Quantum AI. Στην Cirq έμφαση δίνεται στην βελτιστοποίηση των κυκλωμάτων και στην προσαρμογή τους στο ειδικό υλικό των κβαντικών υπολογιστών, που είναι κρίσιμα για την αποδοτική κβαντική υπολογιστική. Αντιμετωπίζει με πιο πραγματικούς όρους την εκτέλεση των κυκλωμάτων, δεδομένου ότι ο θόρυβος που είναι χαρακτηριστικός για τους κβαντικούς υπολογιστές, καθώς και η αρχιτεκτονική τους, καθιστούν συγκεκριμένα κυκλώματα μη εκτελέσιμα πάνω σε συγκεκριμένους κβαντικούς υπολογιστές.

4.6. Εισαγωγή στα κβαντικά LFSR

Στην εποχή της ραγδαίας εξέλιξης της πληροφορικής και της κυβερνοασφάλειας, η κβαντική κρυπτογραφία έχει αναδειχθεί ως ένας κρίσιμος τομέας για την ασφαλή επικοινωνία και την προστασία δεδομένων. Μέσα σε αυτό το πλαίσιο, οι κβαντικές Linear Feedback Shift Registers (LFSR) προσφέρουν μια πρωτοποριακή προσέγγιση για την παραγωγή κρυπτογραφικών κλειδιών, που είναι θεμελιώδη για την ασφάλεια κάθε κρυπτογραφημένου συστήματος.

Οι κβαντικές LFSR διαφοροποιούνται από τις κλασικές μεθόδους στο ότι εκμεταλλεύονται τις κβαντικές ιδιότητες των σωματιδίων, όπως η εμπλοκή και η υπέρθεση για να παράγουν

ακολουθίες κλειδιών με αξιοσημείωτη ασφάλεια. Σε αντίθεση με τις κλασικές LFSR, που χρησιμοποιούν γραμμική ανατροφοδότηση για την παραγωγή ψευδοτυχαίων ακολουθιών, οι κβαντικές LFSR ενσωματώνουν κβαντικές πύλες και εναλλακτικούς μηχανισμούς ανατροφοδότησης που επιτρέπουν τη δημιουργία πιο σύνθετων και δυσδιάκριτων ακολουθιών. Αυτή η ικανότητα να παράγουν ακολουθίες με μεγαλύτερη αντοχή στην κρυπτανάλυση καθιστά τις κβαντικές LFSR ιδιαίτερα πολύτιμες για εφαρμογές κρυπτογραφίας υψηλής ασφάλειας.

Ωστόσο, η κβαντική προσέγγιση αντιμετωπίζει προκλήσεις που προκύπτουν από τις ιδιαιτερότητες της κβαντικής υπολογιστικής, όπως η ανάγκη για υψηλή ακρίβεια στις κβαντικές πύλες και η κβαντική διακύμανση. Η κβαντική διακύμανση, ή decoherence (ΥΠΟΒΑΘΜΙΣΗ-ΣΥΝΑΦΕΙΑΣ) , που αποτελεί την απώλεια κβαντικής πληροφορίας λόγω της αλληλεπίδρασης με το περιβάλλον, αποτελεί μια σημαντική πρόκληση στη διατήρηση της ακεραιότητας των κβαντικών κλειδιών που παράγονται. Επιπλέον, η υλοποίηση κβαντικών πυλών με την απαιτούμενη ακρίβεια και σταθερότητα απαιτεί προηγμένη τεχνολογία και σημαντικούς πόρους, προκαλώντας προκλήσεις τόσο στην κατασκευή όσο και στην πρακτική εφαρμογή των κβαντικών LFSR.

Παρ' όλα αυτά, οι προσπάθειες για την υπέρβαση αυτών των τεχνικών προκλήσεων είναι ενεργές και συνεχίζονται, με την κοινότητα της κβαντικής υπολογιστικής να αναζητά συνεχώς νέες μεθόδους για την βελτίωση της απόδοσης και της ασφάλειας των κβαντικών κρυπτογραφικών συστημάτων. Η εξέλιξη αυτή της κβαντικής κρυπτογραφίας και των κβαντικών LFSR ανοίγει νέους ορίζοντες για την ασφάλεια των δεδομένων στην ψηφιακή εποχή, προσφέροντας προηγμένες λύσεις απέναντι στις εξελισσόμενες απειλές κυβερνοασφάλειας.

4.7. Κβαντικό μητρώο μετατόπισης

Το κβαντικό μητρώο μετατόπισης είναι ένα κβαντικό κύκλωμα το οποίο έχει τη δυνατότητα να μετακινήσει τα qubits προς την πλησιέστερη κατεύθυνση αποφασίζοντας μια συγκεκριμένη κατεύθυνση. Το κύριο συστατικό του κβαντικού μητρώου μετατόπισης QSR είναι οι πύλες ανταλλαγής (SWAP). Η πύλη ανταλλαγής στην ούσια, αποτελείται από τρεις πύλες CNOT. Η ακολουθία των πυλών CNOT που χρησιμοποιείται για να υλοποιήσει μια πύλη SWAP είναι η εξής. Μια πύλη CNOT που έχει ως στόχο το δεύτερο qubit με το πρώτο qubit να λειτουργεί ως ελεγκτής. Μια δεύτερη πύλη CNOT με το πρώτο qubit ως στόχο και το δεύτερο ως ελεγκτή. Μια τρίτη πύλη CNOT που πάλι στοχεύει το δεύτερο qubit με το πρώτο ως ελεγκτή. Αυτή η σειρά εξασφαλίζει ότι οι καταστάσεις των δύο qubits ανταλλάσσονται μεταξύ τους. Η ομορφιά αυτής της μεθόδου έγκειται στην απλότητά της και στην ικανότητά της να χρησιμοποιεί μόνο την πύλη CNOT, μια από τις πιο βασικές κβαντικές πύλες, για την υλοποίηση ενός πιο πολύπλοκου λογικού κυκλώματος όπως το SWAP.

4.8. Κβαντικές πύλες και υλοποίηση LFSR

Η κβαντική έκδοση των LFSR εκμεταλλεύεται τις βασικές κβαντικές πύλες για τη δημιουργία ενός κυκλώματος που μπορεί να παράγει σύνθετες ακολουθίες με υψηλά επίπεδα ασφάλειας. Η κατανόηση των κβαντικών Linear Feedback Shift Registers (QFSR) απαιτεί μια βαθιά κατανόηση των κβαντικών πυλών που χρησιμοποιούνται στην κατασκευή τους, καθώς και τη διαδικασία σχεδίασης τους. Οι κβαντικές πύλες SWAP και C-NOT είναι κρίσιμες στη λειτουργία των κβαντικών LFSR.

Πύλη SWAP

Η χρήση της πύλης SWAP στην υλοποίηση ενός κβαντικού Linear Feedback Shift Register (LFSR) βασίζεται στην ικανότητά της να ανταλλάσσει τις καταστάσεις μεταξύ δύο qubits. Στο πλαίσιο της κβαντικής υλοποίησης του LFSR, αυτή η λειτουργία είναι κρίσιμη για την προσομοίωση της διαδικασίας "shift", που είναι χαρακτηριστική των κλασικών LFSR. Συγκεκριμένα, η πύλη SWAP χρησιμοποιείται για να μετακινήσει κάθε qubit στην επόμενη θέση μέσα στο μητρώο. Σε ένα κβαντικό LFSR, η διαδικασία "shift" που επιτυγχάνεται μέσω των πυλών SWAP είναι κρίσιμη για την ενσωμάτωση της κβαντικής ανατροφοδότησης στο σύστημα. Αυτό σημαίνει ότι η κατάσταση ενός qubit μπορεί να εξαρτάται από τις καταστάσεις άλλων qubits μέσα στο μητρώο, επιτρέποντας τη δημιουργία πολύπλοκων και ασφαλών κρυπτογραφικών ακολουθιών.

Πύλη CNOT

Η πύλη CNOT (Controlled-NOT) χρησιμοποιείται στην υλοποίηση ενός κβαντικού Linear Feedback Shift Register (LFSR) για να επιτύχει την ανατροφοδότηση που είναι κρίσιμη για την παραγωγή των ακολουθιών των ψευδοτυχαίων αριθμών. Στο πλαίσιο του LFSR, η ανατροφοδότηση είναι απαραίτητη για τη διατήρηση της παραγωγής νέων τιμών βάσει των προηγούμενων καταστάσεων των bits. Σε μια κλασική υλοποίηση, αυτό συχνά επιτυγχάνεται μέσω μιας λογικής πράξης XOR.

Στην κβαντική εκδοχή, η πύλη CNOT επιτρέπει την εφαρμογή μιας κβαντικής λογικής πράξης XOR, όπου το δεύτερο qubit (target) αλλάζει κατάσταση μόνο εάν το πρώτο qubit (control) βρίσκεται στην κατάσταση $|1\rangle$. Αυτή η λειτουργία είναι καθοριστική για την επίτευξη της δυναμικής ανατροφοδότησης στο κβαντικό μητρώο, καθώς επιτρέπει την εναλλαγή της κατάστασης ενός qubit βάσει της κατάστασης ενός άλλου qubit.

4.9. Αλγόριθμος κβαντικού LFSR

Ας δημιουργήσουμε λοιπόν βήμα προς βήμα έναν αλγόριθμο Quantum Linear Feedback Shift Register (QLFSR) με 3 qubits.

- Βήμα 1ο: Καθορισμός των Qubits.
  Αρχικά, χρειαζόμαστε 3 qubits (ας τα ονομάσουμε Q0, Q1, και Q2), τα οποία θα είναι τα βασικά στοιχεία του QLFSR μας.
- Βήμα 2ο: Ορισμός αρχικής κατάστασης
  Θέτουμε τα Q0, Q1, και Q2 στις επιθυμητές αρχικές καταστάσεις.
- Βήμα 3ο: Μετατόπιση των qubits
  Εφαρμογή SWAP Gates. Ανταλλάσσουμε τις καταστάσεις των qubits με SWAP gates για να εξομοιώσουμε την διαδικασία μετατόπισης. Για παράδειγμα, SWAP μεταξύ Q0 και Q1, και μετά SWAP μεταξύ Q1 και Q2.
- Βήμα 4ο: Ανάδραση
  Εφαρμόζουμε μια CNOT πύλη για να πραγματοποιήσουμε την λειτουργία XOR βάσει της επιλεγμένης συνάρτησης ανάδρασης. Για παράδειγμα, Q0 (target) και Q3 (control) για να επιτύχουμε την ανάδραση.
- Βήμα 5ο: Έξοδος QLFSR
- Βήμα 6ο: Επανάληψη
  Η διαδικασία μπορεί να επαναληφθεί για να παραχθεί μια σειρά από κβαντικές καταστάσεις που μπορούν να χρησιμοποιηθούν ως κρυπτογραφικά κλειδιά ή για άλλες εφαρμογές. Ας θεωρήσουμε πως η επανάληψη του αλγορίθμο συμβαίνει μέχρι να ξαναφτάσουμε στην αρχικοποιημένη κατάσταση.

4.10. Διαδικασία Σχεδίασης του Κβαντικού LFSR

Η σχεδίαση ενός κβαντικού Linear Feedback Shift Register (LFSR) αποτελεί μια διαδικασία που απαιτεί την ενσωμάτωση κλασικών αρχών LFSR μέσα στο πλαίσιο της κβαντικής υπολογιστικής. Αυτή η διαδικασία μπορεί να διαιρεθεί στα κρίσιμα βήματα που περιγράψαμε παραπάνω και περιλαμβάνουν την επιλογή και αρχικοποίηση των qubits, την εφαρμογή κβαντικών πυλών για την προσομοίωση της ανατροφοδότησης και τη μετατόπιση, και τέλος την προσομοίωση και την ανάλυση των αποτελεσμάτων.

4.10.1. Επιλογή και Αρχικοποίηση των Qubits

Η πρώτη φάση αφορά την επιλογή του αριθμού των qubits που θα χρησιμοποιηθούν στο LFSR. Αυτό καθορίζει το μέγεθος του κβαντικού μητρώου και επηρεάζει την πολυπλοκότητα και την ασφάλεια της παραγόμενης ακολουθίας. Μετά την επιλογή, τα qubits αρχικοποιούνται σε μια συγκεκριμένη κατάσταση, προετοιμάζοντας το έδαφος για την εφαρμογή της ανατροφοδότησης και της μετατόπισης.

4.10.2. Εφαρμογή Κβαντικών Πυλών για Ανατροφοδότηση και Μετατόπιση

Στη συνέχεια, εφαρμόζονται κβαντικές πύλες CNOT και SWAP για την προσομοίωση της ανατροφοδότησης και της διαδικασίας μετατόπισης, αντίστοιχα. Κάνουμε τη δεξιά μετατόπιση μεταξύ των δεδομένων ώστε το q0 πάει στη θέση του q1, και q1 στη θέση του q2, αυτό και το q2 στη θέση του q0. Έτσι το τελευταίο qubit έχει "μετατοπιστεί" στην αρχή του register και τα υπόλοιπα qubits έχουν "σπρώξει" μια θέση προς τα δεξιά. Εφαρμόζουμε, λοιπόν, SWAP μεταξύ q1 και q2 και SWAP μεταξύ q0 και q1. Μετά την μετατόπιση εφαρμόζουμε την κβαντική λειτουργία XOR (εφαρμογή πύλης CNOT) των καταστάσεων συνδεσης. Προκειμένου να παράγουμε μια ακολουθία με μεγαλύτερη πολυπλοκότητα πρέπει να επιλέξουμε καταστάσεις σύνδεσης που επιτυγχάνει τη μεγαλυτερη περίοδο. Οι καταστάσεις σύνδεσης είναι κρίσιμες για την καθορισμό της λειτουργικότητας και της απόδοσης ενός QLFSR, καθώς και για την επίτευξη της μέγιστης περιόδου και των επιθυμητών στατιστικών ιδιοτήτων για την παραγωγή ασφαλών κρυπτογραφικών κλειδιών. Η επιλογή των κατάλληλων καταστάσεων σύνδεσης και η σωστή εφαρμογή των κβαντικών πυλών είναι θεμελιώδεις πτυχές για τη σχεδίαση και την ανάπτυξη αποτελεσματικών κβαντικών κρυπτοσυστημάτων. Αν θεωρήσουμε πως έχουμε ένα μητρωό με n qubits τότε για να υλοποιήσουμε ένα QLFSR χρειαζόμαστε (n-1) πύλες SWAP για την μετατόπιση και μία πύλη CNOT για την ανάδραση. Αυτές οι ενέργειες είναι ζωτικής σημασίας για την αναπαραγωγή της κλασικής λειτουργίας LFSR σε ένα κβαντικό περιβάλλον.

4.10.3 . Προσομοίωση και Ανάλυση

Μετά την εφαρμογή των κατάλληλων πυλών, το κύκλωμα προσομοιώνεται για να παραχθούν και να μετρηθούν οι ακολουθίες των qubits. Η ανάλυση των αποτελεσμάτων επιτρέπει την αξιολόγηση της αποτελεσματικότητας του σχεδιασμού, καθώς και της ασφάλειας της παραγόμενης ακολουθίας.Η διαδικασία σχεδίασης του κβαντικού LFSR απαιτεί μια λεπτομερή κατανόηση τόσο των κβαντικών φαινομένων όσο και των αρχών λειτουργίας των κλασικών LFSR.

4.11 Ανάδραση στα QLFSRs

Όπως είπαμε παραπάνω σε ένα QLFSR, η πύλη CNOT χρησιμοποιείται για να εξομοιώσει την λειτουργία XOR ανάδρασης στα qubits. Η ανάδραση είναι κρίσιμη γιατί χωρίς ανάδραση, η ακολουθία που παράγεται από το QLFSR θα ήταν απλά μια επανάληψη της αρχικής κατάστασης των qubits. Η ανάδραση εισάγει δυναμική που επιτρέπει την παραγωγή μιας πιο περίπλοκης και λιγότερο προβλέψιμης ακολουθίας. Η σωστή εφαρμογή της ανάδρασης μπορεί να αυξήσει την περίοδο της παραγόμενης ακολουθίας, κάτι που είναι ζωτικής σημασίας καθώς δυσκολεύει την πρόβλεψη ή την ανακατασκευή της ακολουθίας.

4.12 Έξοδος του κβαντικού LFSR

Σε έναν κλασικό Linear Feedback Shift Register (LFSR), η έξοδος είναι μια σειρά από bits που προκύπτουν από τη διαδικασία μετατόπισης των bits μέσα στο register και την ανάδραση από ένα ή περισσότερα σημεία του register χρησιμοποιώντας XOR λογική.

Αντίστοιχα, σε έναν Quantum LFSR (QLFSR), η έξοδος δεν είναι μια μονοδιάστατη σειρά bits, αλλά μια κβαντική κατάσταση ή μια σειρά από κβαντικές καταστάσεις που προκύπτουν από αντίστοιχες διαδικασίες εντός του κβαντικού κυκλώματος. Η κβαντική έξοδος είναι συνήθως μια υπέρθεση καταστάσεων, που αποτελείται από πιθανότητες το κάθε qubit να βρεθεί σε μια συγκεκριμένη κατάσταση κατά την μέτρηση.

Η μέτρηση της κβαντικής κατάστασης καταρρέει την υπέρθεση σε μια συγκεκριμένη κατάσταση, και αυτό είναι που παρέχει την "έξοδο" του QLFSR. Αυτή η έξοδος μπορεί να χρησιμοποιηθεί όπως και η έξοδος ενός κλασικού LFSR, για παράδειγμα σε εφαρμογές κρυπτογραφίας ή στην παραγωγή ψευδοτυχαίων αριθμών.

Επειδή οι κβαντικές μετρήσεις είναι πιθανοκρατικές, η έξοδος ενός QLFSR δεν είναι προβλέψιμη με τον ίδιο τρόπο που είναι μια κλασική έξοδος LFSR. Επιπλέον, λόγω της ενδεχόμενης διεμπλοκής μεταξύ των qubits, η πληροφορία για την κατάσταση ενός qubit μπορεί να εξαρτάται από τις καταστάσεις άλλων qubits στο register, κάτι που δεν έχει αντίστοιχο στους κλασικούς LFSRs και αυξάνει την πολυπλοκότητα της ακολουθίας. Το τελικό αποτέλεσμα είναι ότι η έξοδος του QLFSR μπορεί να προσφέρει μια ισχυρότερη μορφή ψευδοτυχαίας ακολουθίας από ό,τι οι κλασικοί LFSR.

4.13 Υλοποίηση 3-qubits QLFSR

Το παρακάτω πρόγραμμα υλοποιεί μια κβαντική γεννήτρια LFSR με τη χρήση της βιβλιοθήκης Cirq της Google και την γλώσσα προγραμματισμού Python.

```
import cirq

def initialize_qubits(qubits, state):
    circuit = cirq.Circuit()
    for i, bit in enumerate(state):
        if bit == '1':
            circuit.append(cirq.X(qubits[i]))
    return circuit

def create_qlfsr_circuit(initial_state):
    qubits = [cirq.LineQubit(i) for i in range(len(initial_state))]
    circuit = initialize_qubits(qubits, initial_state)
    circuit.append(cirq.SWAP(qubits[0], qubits[1]))
    circuit.append(cirq.SWAP(qubits[1], qubits[2]))
    circuit.append(cirq.CNOT(qubits[0], qubits[2]))
    circuit.append(cirq.measure(*qubits, key='m'))
    return circuit

def main():
    initial_state = input("Εισάγετε μια αρχική κατάσταση (π.χ. 101): ")
    simulator = cirq.Simulator()
    current_state = initial_state
    iterations = 0
    states_sequence = [initial_state]  # Λίστα για την αποθήκευση της ακολουθίας των καταστάσεων

    while True:
        circuit = create_qlfsr_circuit(current_state)
        print(f"\nΚύκλωμα στην επανάληψη {iterations}:")
        print(circuit)  # Τύπωμα του κυκλώματος
        result = simulator.run(circuit, repetitions=1)
        measured_state = ''.join(str(bit) for bit in result.measurements['m'][0])
        states_sequence.append(measured_state)  # Αποθήκευση της νέας κατάστασης

        if measured_state == initial_state and iterations > 0:
            print(f"\nΕπέστρεψε στην αρχική κατάσταση μετά από {iterations} επαναλήψεις.")
            print("Ακολουθία καταστάσεων:", " -> ".join(states_sequence))
            break
        else:
            current_state = measured_state
            iterations += 1

if __name__ == "__main__":
    main()
```

4.14. Ανάλυση προγράμματος

- Εισαγωγή Βιβλιοθήκης Cirq: import cirq
  Αυτή η γραμμή κώδικα εισάγει τη βιβλιοθήκη Cirq, η οποία παρέχει τα εργαλεία για τον σχεδιασμό, την προσομοίωση, και την εκτέλεση κβαντικών κυκλωμάτων.
- Αρχικοποίηση Qubits:

```
def initialize_qubits(qubits, state):
    circuit = cirq.Circuit()
    for i, bit in enumerate(state):
        if bit == '1':
            circuit.append(cirq.X(qubits[i]))
    return circuit
```

Η συνάρτηση initialize_qubits παίρνει δύο παραμέτρους: τη λίστα των qubits και την αρχική κατάσταση (σε μορφή συμβολοσειράς). Για κάθε ψηφίο στην αρχική κατάσταση που είναι '1', εφαρμόζεται η πύλη Pauli-X στο αντίστοιχο qubit, φέρνοντάς το στην κατάσταση |1⟩.

- Δημιουργία του Κυκλώματος:

```
def create_qlfsr_circuit(initial_state):
    qubits = [cirq.LineQubit(i) for i in range(len(initial_state))]
    circuit = initialize_qubits(qubits, initial_state)
    circuit.append(cirq.SWAP(qubits[0], qubits[1]))
    circuit.append(cirq.SWAP(qubits[1], qubits[2]))
    circuit.append(cirq.CNOT(qubits[0], qubits[2]))
    circuit.append(cirq.measure(*qubits, key='m'))
    return circuit
```

Η create_qlfsr_circuit δημιουργεί το κβαντικό κύκλωμα για τον QLFSR. Πρώτα, δημιουργεί μια λίστα qubits αντίστοιχη της αρχικής κατάστασης. Στη συνέχεια, αρχικοποιεί τα qubits βάσει της αρχικής κατάστασης και εφαρμόζει σειρά πυλών για την προσομοίωση του QLFSR: SWAP πύλες για την αλλαγή καταστάσεων μεταξύ των qubits και μια CNOT πύλη για την ανάδραση. Τέλος, πραγματοποιείται μέτρηση σε όλα τα qubits και αποθηκεύεται το αποτέλεσμα.

- Main Συνάρτηση:

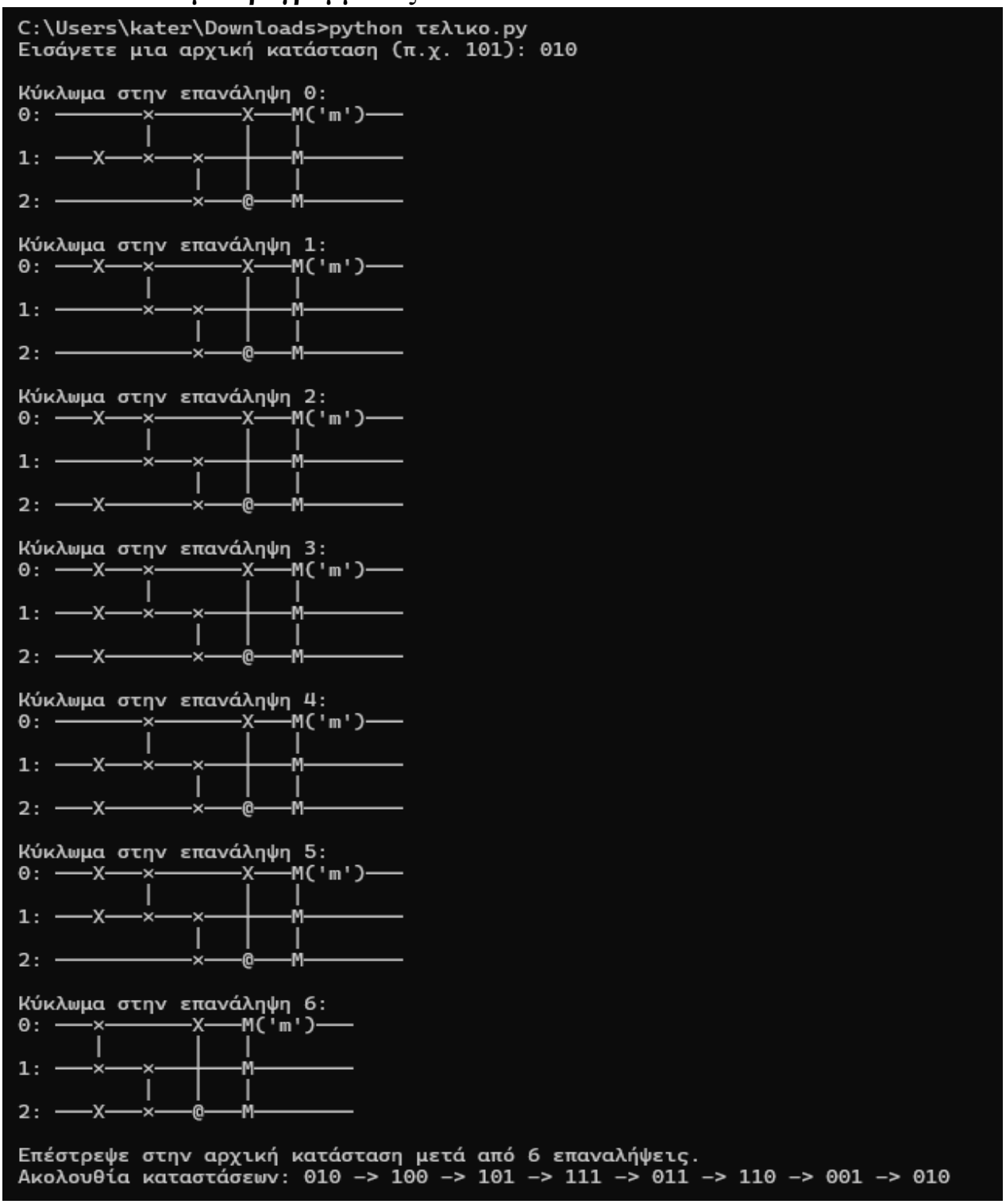
```
def main():
    initial_state = input("Εισάγετε μια αρχική κατάσταση (π.χ. 101): ")
    simulator = cirq.Simulator()
    current_state = initial_state
    iterations = 0
    states_sequence = [initial_state]  # Λίστα για την αποθήκευση της ακολουθίας των καταστάσεων

    while True:
        circuit = create_qlfsr_circuit(current_state)
        print(f"\nΚύκλωμα στην επανάληψη {iterations}:")
        print(circuit)  # Τύπωμα του κυκλώματος
        result = simulator.run(circuit, repetitions=1)
        measured_state = ''.join(str(bit) for bit in result.measurements['m'][0])
        states_sequence.append(measured_state)  # Αποθήκευση της νέας κατάστασης

        if measured_state == initial_state and iterations > 0:
            print(f"\nΕπέστρεψε στην αρχική κατάσταση μετά από {iterations} επαναλήψεις.")
            print("Ακολουθία καταστάσεων:", " -> ".join(states_sequence))
            break
        else:
            current_state = measured_state
            iterations += 1
```

Η main συνάρτηση ξεκινά με την ανάγνωση μιας αρχικής κατάστασης από τον χρήστη και την αρχικοποίηση του προσομοιωτή. Στη συνέχεια, εκτελεί επαναληπτικά το κύκλωμα, μετρά την κατάσταση των qubits μετά από κάθε επανάληψη και αποθηκεύει τις καταστάσεις σε μια λίστα. Αν η μετρηθείσα κατάσταση επανέλθει στην αρχική κατάσταση και έχουν γίνει περισσότερες από μία επαναλήψεις, το πρόγραμμα τερματίζει, εκτυπώνοντας τον αριθμό των επαναλήψεων και την ακολουθία των καταστάσεων που παρήχθησαν.

4.15. Αποτέλεσμα προγράμματος



4.16 Ανάλυση Αποτελεσμάτων

Το πρόγραμμα στην αρχή μας ζητάει να δώσουμε αρχική κατάσταση. Η αρχική κατάσταση που δόθηκε στο παρακάτω παράδειγμα είναι 010. Έπειτα ξεκινάνε οι επαναλήψεις. Στις επαναλήψεις που εκτυπώνονται, βλέπουμε το κύκλωμα που αντιστοιχεί σε κάθε επανάληψη. Κάθε κύκλωμα αποτελείται από τρία qubits, στα οποία εφαρμόζονται διάφορες κβαντικές πύλες όπως οι πύλες X, SWAP και CNOT. Αυτές οι πύλες αλλάζουν την κατάσταση των qubits σε κάθε επανάληψη. Στο τέλος κάθε επανάληψης γίνεται μια μέτρηση της κατάστασης των qubits. Οι μετρήσεις δίνουν τις νέες καταστάσεις 100, 101, 111, 011, 110, 001 και τελικά 010 που είναι ίδια με την αρχική κατάσταση και έτσι τερματίζει το πρόγραμμα. Αυτή η ακολουθία φαίνεται να είναι το αποτέλεσμα της προσομοίωσης του LFSR. Το πρόγραμμα εκτυπώνει ότι η αρχική κατάσταση επέστρεψε μετά από 6 επαναλήψεις, πράγμα που δείχνει την περιοδικότητα της ακολουθίας που παράγεται. Στην κβαντική προσομοίωση, αυτό σημαίνει ότι μετά από έναν συγκεκριμένο αριθμό επαναλήψεων, το σύστημα επανέρχεται στην αρχική κατάσταση. Για ένα QLFSR με τρία qubits, υπάρχουν μόνο $2^3 = 8$ δυνατές καταστάσεις. Αυτό σημαίνει ότι ο χώρος των δυνατών καταστάσεων είναι αρκετά περιορισμένος, και οι επαναλήψεις μέσω αυτού του χώρου θα οδηγήσουν σχετικά γρήγορα σε επανάληψη.

4.17 Ακολουθίες που παράγονται από το QLFSR

Η βασική διαφορά μεταξύ των κβαντικών Linear Feedback Shift Registers (QLFSR) και των κλασικών LFSR αναφέρεται κυρίως στον τρόπο λειτουργίας και στην φύση των ακολουθιών που παράγουν. Στα κλασικά LFSR, η κάθε επόμενη κατάσταση του συστήματος προκύπτει από την προηγούμενη με την εφαρμογή μιας γραμμικής συνάρτησης. Αυτό σημαίνει ότι, αν κάποιος γνωρίζει μια αρκετά μεγάλη σειρά από τιμές της ακολουθίας, μπορεί να υπολογίσει τις επόμενες τιμές. Οι ακολουθίες που παράγονται είναι περιοδικές και η περίοδος εξαρτάται από την αρχική κατάσταση και τη συνάρτηση ανάδρασης. Στην κβαντική εκδοχή των LFSR, τα πράγματα γίνονται πιο περίπλοκα λόγω της υπερθέσης και της διεμπλοκής των κβαντικών καταστάσεων. Σε ένα κβαντικό LFSR, τα qubits μπορούν να βρίσκονται σε υπερθέσεις καταστάσεων, επιτρέποντας την παραγωγή ακολουθιών που είναι πολύ πιο περίπλοκες από αυτές που μπορούν να παραχθούν από κλασικά LFSR.

Η διαφορά στις ακολουθίες που παράγονται αναφέρεται κυρίως στο γεγονός ότι τα κβαντικά LFSR μπορούν να εκμεταλλευτούν την κβαντική υπερθέση για να παράγουν ακολουθίες σε ένα ευρύ φάσμα πιθανών καταστάσεων ταυτόχρονα, αντί για μία μόνο κατάσταση ανά στιγμή όπως στα κλασικά LFSR. Αυτό μπορεί να οδηγήσει σε ακολουθίες με πολύ υψηλότερο επίπεδο πολυπλοκότητας και ασφάλειας, καθώς η προβλεψιμότητα και η περιοδικότητα των κλασικών LFSR μπορεί να εξαλειφθεί χάρη στις κβαντικές ιδιότητες.

- *Αλγόριθμος Berlekamp-Massey στα κλασικά και κβαντικά LFSR*

  Στα κλασικά LFSR που αποτελούνται από N καταχωρητές και η περίοδος είναι $2^N - 1$, σύμφωνα με το θεώρημα Berlekamp-Massey η παρατήρηση διαδοχικών N εξόδων από το LFSR επιτρέπει την αποκάλυψη του πολύωνυμου ανάδρασης. Για κάθε δοθείσα ακολουθία πεπερασμένου μήκους $s_1, s_2, \dots, s_N$ υπάρχει ένα ελάχιστο πολυώνυμο ανάδρασης $L(x)$ που την παράγει, και ο αλγόριθμος Berlekamp-Massey μπορεί να το βρει αποδοτικά. Αυτό το πολυώνυμο $L(x)$ είναι το πολυώνυμο μη μηδενικού ελάχιστου βαθμού τέτοιο ώστε:

  $L(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_L x^L$ με $c_0 = 1$ που ικανοποιεί τη σχέση:
  $s_{j+1} = c_1 s_j + c_2 s_{j-1} + \cdots + c_L s_{j-L+1}$ για $j = L, L+1, \dots, n-1$

  Η κατασκευή του $L(x)$ γίνεται επεξεργάζοντας την ακολουθία από την αρχή προς το τέλος. Για κάθε νέο στοιχείο, υπολογίζεται η διαφορά μεταξύ της παρατηρούμενης και της προβλεπόμενης τιμής. Αν αυτή η διαφορά είναι μη μηδενική, το πολυώνυμο ανανεώνεται. Κάθε φορά που υπάρχει σφάλμα (δηλαδή η διαφορά δεν είναι μηδέν), το τρέχον πολυώνυμο $L(x)$ ανανεώνεται χρησιμοποιώντας έναν παράγοντα διόρθωσης που εξαρτάται από το σφάλμα και την προηγούμενη τιμή του $L(x)$. Αυτό συμβάλλει στη μείωση του συνολικού σφάλματος στις επόμενες προβλέψεις. Το αποτέλεσμα μετά την επεξεργασία όλων των στοιχείων της ακολουθίας είναι το $L(x)$, το οποίο είναι το ελάχιστο πολυώνυμο ανάδρασης που περιγράφει πλήρως την ακολουθία και μπορεί να χρησιμοποιηθεί για να προβλέψει ή να ανακατασκευάσει την ακολουθία από οποιοδήποτε σημείο.

  Η προσπάθεια υλοποίησής του αλγόριθμου Berlekamp-Massey σε ένα κβαντικό περιβάλλον, όπως σε ένα κβαντικό LFSR (QLFSR), συναντά σημαντικά εμπόδια. Ο αλγόριθμος Berlekamp-Massey είναι επαγωγικός και αναδρομικός, ενημερώνοντας το ελάχιστο πολυώνυμο βάσει των τρεχουσών παρατηρήσεων και των προηγούμενων σφαλμάτων. Στην κβαντική υπολογιστική, όλες οι πύλες (εκτός από τη μέτρηση) είναι αναστρέψιμες. Αυτό σημαίνει ότι για να υλοποιήσουμε μια λογική πράξη στα κβαντικά κυκλώματα, χρειαζόμαστε να διατηρήσουμε πλήρως την πληροφορία για κάθε κβαντική κατάσταση, χωρίς να επιτρέπουμε την απώλεια ή την καταστροφή πληροφορίας. Στον Berlekamp-Massey, η ανάγκη για συνεχείς αναδρομικές ενημερώσεις και η δυνατότητα καταστροφής ή απώλειας πληροφορίας στις διορθώσεις σφαλμάτων δεν μπορούν να αναπαρασταθούν αποτελεσματικά με αναστρέψιμες πύλες.

  Επιπλέον ο αλγόριθμος Berlekamp-Massey βασίζεται στη γραμμική αναδρομή για να προσδιορίσει το ελάχιστο πολυώνυμο. Αυτή η γραμμική αναδρομή υπολογίζει τις τιμές

βασιζόμενες σε προηγούμενα δεδομένα και κάνει επαναληπτικές ενημερώσεις του πολυωνύμου. Σε ένα κβαντικό περιβάλλον, οι ακολουθίες δεν είναι απλές καταστάσεις αλλά υπερθέσεις καταστάσεων. Η επεξεργασία κάθε στοιχείου ανεξάρτητα, χωρίς να επηρεάζεται η υπέρθεση των άλλων, είναι εξαιρετικά δύσκολη. Η αναδρομική διαδικασία που χρησιμοποιεί ο Berlekamp-Massey, απαιτώντας συγκεκριμένες τιμές και ενημερώσεις, αντιβαίνει στη φύση της κβαντικής υπέρθεσης και εμπλοκής.

Ο αλγόριθμος Berlekamp-Massey απαιτεί την επαλήθευση και την πιθανή διόρθωση κάθε στοιχείου της ακολουθίας. Στην κβαντική υπολογιστική, η μέτρηση ενός qubit προκαλεί τον κατάρρευση σε συγκεκριμένη κβαντική κατάσταση χάνοντας όλες τις άλλες πληροφορίες. Για τον Berlekamp-Massey, αυτό σημαίνει ότι οποιαδήποτε προσπάθεια μέτρησης ή επαλήθευσης του ενδιάμεσου αποτελέσματος θα κατέρρεε την κβαντική υπέρθεση και θα έκανε αδύνατη την συνέχιση του αναδρομικού υπολογισμού.

Συμπερασματικά ο αλγόριθμος Berlekamp-Massey υπολογίζει το ελάχιστο πολυώνυμο ανάδρασης μέσω ενός κλασικού αναδρομικού μηχανισμού που δεν μπορεί να μεταφραστεί απευθείας στην κβαντική υπολογιστική λόγω της ανάγκης για αναστρεψιμότητα, διατήρηση της υπέρθεσης και της εμπλοκής, και του περιορισμού των κβαντικών μετρήσεων που καταρρέουν την κβαντική κατάσταση.

- *Αν κάνουμε διαδοχικά ανακυκλώσεις στην περίπτωση του QLFSR στις μετρήσεις προκύπτουν κάθε φορά διαφορετικές αλληλουχίες ή όχι;*

Στην κβαντική υπολογιστική, οι μετρήσεις ενός κβαντικού συστήματος έχουν μια ιδιαίτερη ιδιότητα που τις διαφοροποιεί από τις κλασικές μετρήσεις: κάθε μέτρηση επηρεάζει την κατάσταση του συστήματος. Συγκεκριμένα, όταν μετράμε την κατάσταση ενός κβαντικού συστήματος που βρίσκεται σε υπέρθεση, η κυματοσυνάρτηση του συστήματος "καταρρέει" σε μία από τις δυνατές καταστάσεις με μια πιθανότητα που προκύπτει από την υπέρθεση. Όταν λοιπόν πραγματοποιούμε διαδοχικές μετρήσεις σε ένα κβαντικό σύστημα, η απάντηση στο ερώτημα εάν οι ακολουθίες των αποτελεσμάτων θα είναι διαφορετικές κάθε φορά εξαρτάται από τον τρόπο με τον οποίο το σύστημα προετοιμάζεται πριν από κάθε μέτρηση. Αν το σύστημα προετοιμάζεται με τον ίδιο τρόπο πριν από κάθε μέτρηση, τότε μπορεί να παραχθεί μια παρόμοια σειρά αποτελεσμάτων για κάθε μέτρηση, υπό την προϋπόθεση ότι η προετοιμασία είναι ακριβής και επαναλαμβάνεται άψογα. Ωστόσο, λόγω της πιθανοκρατικής φύσης των μετρήσεων στην κβαντική μηχανική, ακόμη και με την ίδια προετοιμασία, τα αποτελέσματα μπορεί να διαφέρουν από μέτρηση σε μέτρηση. Αν το σύστημα δεν προετοιμάζεται εκ νέου μεταξύ

των μετρήσεων, τότε οι διαδοχικές μετρήσεις θα εξαρτώνται από την κατάσταση που άφησε η προηγούμενη μέτρηση, οδηγώντας σε διαφορετικά αποτελέσματα κάθε φορά.

Σε γενικές γραμμές, δεδομένης της κβαντικής αρχής της αβεβαιότητας και του καταρρεύσεως της κυματοσυνάρτησης κατά την μέτρηση, ακόμα και με ίδια προετοιμασία, δεν είναι εγγυημένο ότι οι διαδοχικές ανακυκλώσεις θα παράγουν την ακριβώς ίδια ακολουθία αποτελεσμάτων σε κάθε επανάληψη. Αυτό καθιστά τις κβαντικές μετρήσεις ένα πολύτιμο εργαλείο για εφαρμογές όπως η κβαντική κρυπτογραφία, όπου η αβεβαιότητα και η απρόβλεπτη φύση των αποτελεσμάτων μπορούν να εξυπηρετήσουν ως μια μορφή ασφάλειας.

- *Τι συμβαίνει όμως στην υλοποίηση που περιγράψαμε παραπάνω;*

  Ο κώδικας προετοιμάζει τα qubits με τον ίδιο τρόπο πριν από κάθε μέτρηση, αυτό σημαίνει ότι επαναφέρει το σύστημα σε μια συγκεκριμένη αρχική κατάσταση πριν από την εκτέλεση των μετρήσεων. Πιο συγκεκριμένα η συνάρτηση initialize_qubits(qubits, state) αρχικοποιεί τα qubits στην επιθυμητή αρχική κατάσταση βάσει της συμβολοσειράς state που παρέχεται ως είσοδος. Αν η τιμή ενός bit είναι '1', τότε εφαρμόζεται η πύλη X (συνάρτηση NOT) στο αντίστοιχο qubit για να το φέρει στην κατάσταση |1⟩. Η συνάρτηση create_qlfsr_circuit(initial_state) δημιουργεί και επιστρέφει ένα κύκλωμα που υλοποιεί τη λειτουργία ενός QLFSR βάσει της αρχικής κατάστασης initial_state. Το κύκλωμα περιλαμβάνει πύλες SWAP και CNOT, και καταλήγει σε μια μέτρηση των qubits. Στην κύρια συνάρτηση main(), το πρόγραμμα εισάγει μια αρχική κατάσταση, και στη συνέχεια εκτελεί επαναληπτικά το κύκλωμα QLFSR, αποθηκεύοντας και τυπώνοντας την ακολουθία των καταστάσεων που παράγονται. Μετά από κάθε εκτέλεση, το πρόγραμμα χρησιμοποιεί την μετρημένη κατάσταση ως την "νέα αρχική κατάσταση" για την επόμενη επανάληψη, μέχρι να επιστρέψει στην αρχική κατάσταση.

  Τρέχοντας τον κώδικα αυτό οι ακολουθίες που παράγονται για κάθε αρχική κατάσταση είναι ίδιες. Το αποτέλεσμα αυτό όπου οι ακολουθίες που παράγονται από το πρόγραμμα είναι οι ίδιες σε κάθε εκτέλεση, είναι συμβατή με την ιδέα ότι ο κβαντικός υπολογιστής (ή στην πραγματικότητα ο κβαντικός προσομοιωτής σε αυτή την περίπτωση) αρχικοποιεί τα qubits σε μια συγκεκριμένη κατάσταση πριν από κάθε σειρά μετρήσεων. Αυτό είναι σύμφωνο με την πρώτη περίπτωση που αναφέρεται παραπάνω, όπου το σύστημα προετοιμάζεται με τον ίδιο τρόπο πριν από κάθε μέτρηση. Προσθετικά, ένας ακόμα παράγοντας που καθορίζει τις ακολουθίες που παράγονται είναι ο προσομοιωτής που χρησιμοποιούμε. Όταν χρησιμοποιούμε έναν κβαντικό προσομοιωτή όπως ο Cirq για να προσομοιώσουμε έναν QLFSR, είμαστε περιορισμένοι στις δυνατότητες και τις παραδοχές του λογισμικού. Αυτό μπορεί να μην αποτυπώνει πλήρως τις δυνατότητες ενός

πραγματικού κβαντικού υπολογιστή. Η "τυχαιότητα" στις μετρήσεις ελέγχεται από τον αλγόριθμο του προσομοιωτή και όχι από πραγματικές κβαντικές διαδικασίες. Αυτό σημαίνει ότι, υπό τις ίδιες συνθήκες, ο προσομοιωτής θα παράγει τα ίδια αποτελέσματα κάθε φορά.

- *Οι ακολουθίες που παράγονται από τον qlfsr είναι αυτές που παράγονται στο κλασσικό lfsr;*

  Η παραγωγή ίδιων ακολουθιών από ένα QLFSR και έναν κλασικό LFSR θα απαιτούσε κάποια μορφή αντιστοιχίας μεταξύ των πολυωνύμων ανάδρασης που χρησιμοποιούνται στις δύο διαφορετικές υλοποιήσεις. Τα πολυώνυμα ανάδρασης καθορίζουν πώς οι τρέχουσες καταστάσεις των registers (ή qubits, στην περίπτωση των QLFSR) επηρεάζουν την επόμενη κατάσταση του συστήματος.

  Στον κλασικό LFSR, το πολυώνυμο ανάδρασης είναι καθορισμένο από τη θέση των taps, δηλαδή των σημείων στα οποία οι εξόδοι από συγκεκριμένους καταχωρητές ανατροφοδοτούνται πίσω στο σύστημα μέσω μιας XOR πύλης. Το πολυώνυμο ανάδρασης ουσιαστικά καθορίζει την περιοδικότητα και την ποικιλομορφία των ακολουθιών που μπορούν να παραχθούν.

  Στον QLFSR, η έννοια του πολυωνύμου ανάδρασης μπορεί να μεταφραστεί σε ένα ανάλογο σύνολο κβαντικών πυλών που εφαρμόζονται σε ένα σύστημα qubits, με σκοπό να προσομοιώσει την ανάδραση που παρατηρείται σε κλασικούς LFSR. Αυτό μπορεί να περιλαμβάνει τη χρήση πυλών όπως οι CNOT για την εκτέλεση κβαντικών λογικών επιχειρήσεων που αντιστοιχούν στις κλασικές XOR λειτουργίες, καθώς και πυλών SWAP για την αλλαγή της θέσης των qubits.

  Για να προσδιορίσουμε το αντίστοιχο κλασικό LFSR του QLFSR που υλοποιήσαμε με χρήση της Cirq, εξετάζουμε τις πύλες και τις λειτουργίες που εφαρμόζονται στο κύκλωμα. Πύλες SWAP μεταξύ των qubits 0 και 1, και των qubits 1 και 2. Αυτό αλλάζει τη θέση των qubits στο κύκλωμα. Πύλη CNOT μεταξύ των qubits 0 και 2, όπου το qubit 0 λειτουργεί ως ελεγκτής και το qubit 2 ως στόχος. Αυτή η επιχείρηση εφαρμόζει μια κατάσταση XOR μεταξύ των δύο qubits. Το αντίστοιχο κλασικό LFSR που περιγράφεται από τον κώδικά θα έχει ένα πολυώνυμο ανάδρασης που ενσωματώνει τη λειτουργία XOR μεταξύ των τρίτου και πρώτου bits και δεξιά ολίσθηση των bits και εισαγωγή του αποτελέσματος της XOR στο αρχικό bit. Ένα αντίστοιχο κλασικό LFSR με βάση όσα περιγράψαμε θα έχει την παρακάτω μορφή. Ένα 3-bit LFSR με ταπ στην τρίτη και πρώτη θέση. Το ταπ στο τρίτο bit χρησιμοποιείται για να εφαρμοστεί ανάδραση XOR στο πρώτο bit πριν από τη μετατόπιση. Παρακάτω ο κώδικας που υλοποιεί το κλασικό LFSR:

```
start_state = 0b101  # Αρχική κατάσταση των 3 bits
lfsr = start_state
period = 0
sequence = []  # Λίστα για την αποθήκευση της ακολουθίας των καταστάσεων

while True:
    sequence.append(f'{lfsr:03b}')  # Προσθήκη της τρέχουσας κατάστασης στη λίστα με μορφοποίηση σε δυαδικό με προηγούμενα μηδενικά
    # taps: 3 1; feedback polynomial: x^3 + x + 1
    bit = (lfsr ^ (lfsr >> 2)) & 1  # XOR μεταξύ του τρίτου και του πρώτου bit
    lfsr = (lfsr >> 1) | (bit << 2)  # Μετατόπιση δεξιά και εισαγωγή του νέου bit στην αριστερή πλευρά
    period += 1
    if lfsr == start_state:
        sequence.append(f'{lfsr:03b}')  # Προσθήκη της τελικής κατάστασης στη λίστα
        print(f"Η ακολουθία που παράγεται είναι: {' -> '.join(sequence)}")
        print(f"Περίοδος: {period}")
        break
```

Τρέχοντας τόσο το κβαντικό όσο και το κλασικό LFSR τα αποτελέσματα που παράγονται είναι διαφορετικά. Αυτή η διαφορά οφείλεται στις θεμελιώδεις διαφορές μεταξύ της κλασικής και της κβαντικής υπολογιστικής, καθώς και στη διαφορετική φύση της πληροφορίας και των εντολών σε κάθε περίπτωση όπως περιγράψαμε και παραπάνω.

4.18 Αποκάλυψη Πολυωνύμου Ανάδρασης

- *Η χρήση ενός Quantum Linear Feedback Shift Register N qubits θα μπορούσε να αποκαλύψει το πολυώνυμο ανάδρασης ενός κλασικού LFSR, οι ακολουθίες του οποίου εισάγονται στον QLFSR;*

  Πρώτα απ' όλα, είναι σημαντικό να σημειωθεί ότι οι κβαντικοί και οι κλασικοί υπολογιστές λειτουργούν σε διαφορετικές αρχές. Ένας QLFSR εκμεταλλεύεται κβαντικές ιδιότητες όπως η υπέρθεση και η διεμπλοκή, οι οποίες δεν έχουν αντίστοιχο στον κλασικό υπολογισμό. Αυτό σημαίνει ότι η απλή "μετάφραση" των εξόδων ενός κλασικού LFSR σε εισόδους για έναν QLFSR μπορεί να μην είναι αρκετή για να αποκαλύψει απευθείας τις λεπτομέρειες του πολυωνύμου ανάδρασης του κλασικού LFSR. Για να χρησιμοποιήσουμε έναν QLFSR για την αναγνώριση ή αποκάλυψη του πολυωνύμου ανάδρασης ενός κλασικού LFSR, θα χρειαστεί να ενσωματώσουμε ειδικούς αλγορίθμους ή τεχνικές που εκμεταλλεύονται τις μοναδικές ιδιότητες του κβαντικού υπολογισμού.

Ο αλγόριθμος αναζήτησης του Grover θα μπορούσε να είναι χρήσιμος για την αναζήτηση του σωστού πολυωνύμου ανάδρασης από ένα σύνολο υποψηφίων. Αυτό απαιτεί τον ορισμό μιας συνάρτησης "ελέγχου" η οποία θα δέχεται ως είσοδο ένα πιθανό πολυώνυμο και θα ελέγχει αν παράγει την ίδια ακολουθία με τον κλασικό LFSR. Ο αλγόριθμος του Grover μπορεί να επιταχύνει σημαντικά την αναζήτηση στο σωστό πολυώνυμο ανάδρασης σε σύγκριση με κλασικές μεθόδους.

Η δημιουργία και η εφαρμογή μιας συνάρτησης "ελέγχου" για την κβαντική αναζήτηση, που θα εξετάζει πιθανά πολυώνυμα ανάδρασης για έναν LFSR, είναι μια σύνθετη διαδικασία που περιλαμβάνει πολλά βήματα. Μία προσέγγιση είναι να δημιουργήσουμε ένα προκαθορισμένο σύνολο πιθανών πολυωνύμων ανάδρασης βάσει των γνωστών χαρακτηριστικών των LFSR. Για παράδειγμα, σε ένα 3-bit LFSR, μπορούμε να εξετάσουμε όλους τους δυνατούς συνδυασμούς taps που θα μπορούσαν να οδηγήσουν σε μέγιστη περίοδο. Θα δημιουργήσουμε, λοιπόν, ένα προκαθορισμένο σύνολο πιθανών πολυωνύμων. Η δημιουργία ενός συνόλου υποψήφιων πολυωνύμων που είναι επαρκώς αντιπροσωπευτικό και διαχειρίσιμο σε μέγεθος έχει μεγάλη πολυπλοκότητα.

Χωρίς τη χρήση εξειδικευμένων αλγορίθμων ή συγκεκριμένων τεχνικών ανάλυσης, ένας Quantum LFSR (QLFSR) καθ' εαυτόν δεν είναι πιθανό να μπορέσει να αποκαλύψει άμεσα το πολυώνυμο ανάδρασης ενός κλασικού LFSR. Οι κβαντικοί και κλασικοί υπολογιστές λειτουργούν βάσει διαφορετικών αρχών. Αυτή η θεμελιώδης διαφορά στην υπολογιστική λογική καθιστά δύσκολη την άμεση "μετάφραση" ή αποκάλυψη των χαρακτηριστικών του ενός συστήματος από το άλλο χωρίς επιπλέον επεξεργασία. Ένας QLFSR, ενώ μπορεί να προσομοιώσει τις δυναμικές ενός κλασικού LFSR σε κβαντικό επίπεδο, η απλή λειτουργία του δεν παρέχει απευθείας τα μέσα για την αποκάλυψη του πολυωνύμου ανάδρασης που χρησιμοποιεί ο κλασικός LFSR.

Οι κβαντικοί υπολογιστές δεν "αντιλαμβάνονται" απευθείας την κλασική ανάδραση ως τέτοια. Η ανάδραση στον κλασικό LFSR εξαρτάται από την ακολουθία των δυαδικών χειρισμών που είναι προκαθορισμένοι και γραμμικοί, ενώ σε ένα QLFSR η υπέρθεση και η διεμπλοκή δεν οδηγούν απευθείας σε ένα συγκεκριμένο πολυώνυμο ανάδρασης χωρίς επιπρόσθετη ανάλυση. Επιπλέον η αποκωδικοποίηση πληροφορίας από κβαντικές μετρήσεις είναι σύνθετη και απαιτεί προηγμένους αλγορίθμους και μεθόδους για να ερμηνευθούν οι κβαντικές καταστάσεις σε κλασικά δεδομένα.

Βιβλιογραφία

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.

[2] A. J. *et al.*, "Quantum Algorithm Implementations for Beginners," *ACM Transactions on Quantum Computing*, Mar. 2022, doi: https://doi.org/10.1145/3517340.

[3] "Linear Feedback Shift Register - an overview | ScienceDirect Topics," *www.sciencedirect.com*. https://www.sciencedirect.com/topics/mathematics/linear-feedback-shift-register

[4] Wikipedia Contributors, "Linear-feedback shift register," *Wikipedia*, Nov. 06, 2019. https://en.wikipedia.org/wiki/Linear-feedback_shift_register

[5] H.-I. Kim and J.-C. Jeon, "Quantum LFSR Structure for Random Number Generation Using QCA Multilayered Shift Register for Cryptographic Purposes," *Sensors*, vol. 22, no. 9, pp. 3541–3541, May 2022, doi: https://doi.org/10.3390/s22093541.

[6] "IBM Quantum," *IBM Quantum*. https://quantum.ibm.com/

[7] "Google Quantum AI," *Google Quantum AI*. https://quantumai.google/

[8] R. Z. Khalaf and A. A. Abdullah, "Generate Quantum Key by Using Quantum Shift Register," International Journal of Computer Networks and Communications Security, vol. 3, no. 6, pp. 248-252, June 2015.

[9] "Cirq," *Google Quantum AI*. https://quantumai.google/cirq

[10] Wikipedia Contributors, "Berlekamp–Massey algorithm," *Wikipedia*, Oct. 19, 2023. https://en.wikipedia.org/wiki/Berlekamp%E2%80%93Massey_algorithm (accessed Jun. 01, 2024).

[11] Β. Ε. Μουλός, "Κβαντικοί Υπολογισμοί Και Κβαντικός Προγραμματισμός," *Ntua.gr*, Jul. 2014, doi: http://artemis-new.cslab.ece.ntua.gr:8080/jspui/handle/123456789/16931.

[12] Μιχαήλ Λαμπής, "Γλώσσες Κβαντικού Προγραμματισμού Θεωρία Και Υλοποίηση," *Ntua.gr*, Dec. 2005, doi: http://artemis-new.cslab.ece.ntua.gr:8080/jspui/handle/123456789/14377.